Domain

1

Monitoring and Reporting

1. You are a system administrator and you need to view the metrics that are available in the Amazon EC2 instance namespace. What command can you type into the Amazon CLI?
   - **A.** `aws cloudwatch list-instances --namespace AWS/EC2`
   - **B.** `aws cloudwatch list-metrics --name AWS/EC2`
   - **C.** `aws cloudwatch list-metrics --namespace AWS/EC2`
   - **D.** `aws cloudwatch list-instances --name AWS/EC2`
2. Where can you look up metrics that are available in Amazon CloudWatch?
   - **A.** EC2 Console
   - **B.** CloudWatch Console
   - **C.** CloudTrail Console
   - **D.** Trusted Advisor Console
3. How can you access Amazon CloudWatch?
   - **A.** Amazon CloudWatch Console
   - **B.** AWS CLI
   - **C.** CloudWatch API
   - **D.** All of the above
4. Which service can use Amazon CloudWatch alarms to increase or decrease capacity based on compute load (CPU utilization, etc.)?
   - **A.** AWS Lambda
   - **B.** Amazon S3
   - **C.** Amazon EC2 Auto Scaling
   - **D.** Amazon VPC
5. Which of the following are valid alarm states for Amazon CloudWatch? (Choose three.)
   - **A.** ALARM
   - **B.** OK
   - **C.** READY
   - **D.** INSUFFICIENT_DATA
   - **E.** OFFLINE
   - **F.** WARNING
6. You have been asked to create Amazon CloudWatch alarms for each of your organization's 600 servers, which all reside within the same region. Assuming you create five alarms per server, will you be able to create alarms for each of the servers?
   - **A.** Yes, because the limit is 5000 alarms per region.
   - **B.** Yes, because the limit is 3500 alarms per region.
   - **C.** Yes, because the limit is 10,000 alarms per region.
   - **D.** No, you can't create that many alarms in a single region.

7. You are a system administrator at your company, and you have been asked to check why an existing Amazon CloudWatch alarm is showing INSUFFICIENT_DATA for one of your established servers. What is the best explanation for why this is occurring?
   - **A.** CloudWatch is experiencing an outage.
   - **B.** Not enough data is available for the metric to determine whether it should be OK or ALARM.
   - **C.** The alarm has only just been started, so it doesn't have enough data to determine if the state should be OK or ALARM.
   - **D.** The server is offline so no metrics are available.

8. You are a system administrator at your company, and you have been asked to check why a new Amazon CloudWatch alarm is showing INSUFFICIENT_DATA for one of your established servers. What is the best explanation for why this is occurring?
   - **A.** CloudWatch is experiencing an outage.
   - **B.** Not enough data is available for the metric to determine whether it should be OK or ALARM.
   - **C.** The alarm has only just been started, so it doesn't have enough data to determine if the state should be OK or ALARM.
   - **D.** The server is offline so no metrics are available.

9. Your bosses have come to you and have asked you if there is a way for them to get real-time notifications if a certain Amazon CloudWatch alarm is triggered. What should your bosses do to ensure that they can get real-time notifications? The answer should minimize administrative overhead.
   - **A.** Subscribe to an SNS topic that will send an SMS text message when the Amazon CloudWatch alarm is triggered.
   - **B.** Write a custom AWS Lambda function that will send an email when the Amazon CloudWatch alarm is triggered.
   - **C.** Use an SQS queue to deliver messages when an Amazon CloudWatch alarm is triggered.
   - **D.** Use a third-party solution to send notifications via SMS text message when an Amazon CloudWatch alarm is triggered.

10. You need to set up an Amazon CloudWatch alarm that will trigger after four failed evaluations of the alarm metrics in a 5-minute period. What do you need to set the evaluation period and the data points to alarm to so that you get the desired result?
    - **A.** Data points to alarm should be set to 5. Evaluation period should be set to 1 minute.
    - **B.** Data points to alarm should be set to 4. Evaluation period should be set to 5 minutes.
    - **C.** Data points to alarm should be set to 5. Evaluation period should be set to 5 minutes.
    - **D.** Data points to alarm should be set to 4. Evaluation period should be set to 1 minute.

11. Your boss has asked you to ensure that the 5-minute data points from CloudWatch are available for at least 60 days. What do you need to change within Amazon CloudWatch to ensure that you have at least 60 days' worth of 5-minute data points?

A. Nothing, Amazon CloudWatch can't retain data points that long.

B. Nothing. By default, Amazon CloudWatch keeps 5-minute data points for 63 days.

C. Create an archive to maintain 5-minute data points for at least 60 days.

D. Set Amazon CloudWatch to never delete the 5-minute data points.

12. What is a namespace in Amazon CloudFront?

A. A logical grouping of Amazon CloudWatch metrics

B. A logical grouping of Amazon CloudWatch alerts

C. A logical grouping of Amazon CloudWatch logs

D. A logical grouping of report names for Amazon CloudWatch

13. In which Amazon CloudWatch namespace would the metrics for EC2 be located?

A. AWS/ELB

B. AWS/EBS

C. AWS/EC2

D. AWS/Auto Scaling

14. In which Amazon CloudWatch namespace would the metrics for an Application Load Balancer be located?

A. AWS/ELB

B. AWS/ApplicationELB

C. AWS/EBS

D. AWS/Auto Scaling

15. You have been asked to retrieve some statistics from Amazon CloudWatch for a production server that is having issues. Your organization uses dimensions to further identify custom metrics. You know that the published dimension for the metric contains the following:

Dimensions: Server=Production, Site=Location1

Which of the following could be used to retrieve the statistics that you need?

A. Server=Production

B. Server=Production, Site=Location

C. Server=Prod

D. Server=Production, Site=Location1

16. Which of these Amazon EC2 metrics require that an agent be installed on the server so that Amazon CloudWatch can gather the statistics for the system?

A. Disk performance

B. Network utilization

C. Memory utilization

D. CPU utilization

17. When using Amazon CloudWatch, there are two types of health checks used for EC2 instances. Which of the following options are valid status checks? (Choose two.)

A. Performance status check

B. System status check

C. Health status check

D. Virtual machine status check

E. Instance status check

18. You are a system administrator for a mid-size financial institution. You are checking the health of your company's assets when you notice that CloudWatch is indicating that one of your EC2 instances has failed its instance status check. Which of the following is a possible cause?

A. Exhausted memory

B. Incompatible application installed

C. Software license key has expired.

D. Wrong OS is installed.

19. You are a system administrator for a mid-size financial institution. You are checking the health of your company's assets when you notice that CloudWatch is indicating that one of your EC2 instances has failed its instance status check. Which of the following is a possible cause?

A. Wrong OS is installed.

B. The filesystem is NTFS.

C. Corrupted filesystem

D. The filesystem is ext4.

20. You are a system administrator for a mid-size financial institution. You are checking the health of your company's assets when you notice that CloudWatch is indicating that one of your EC2 instances has failed its instance status check. Which of the following is a possible cause?

A. IPv4 is enabled.

B. Subnet is too large.

C. Wrong OS is installed.

D. Incorrect network configurations

21. You want to check the status of your Amazon EC2 instances. What is the command that you would enter into the AWS CLI to check the status of your instances?

A. `aws cloudfront check-instance-status`

B. `aws cloudfront describe-instance-status`

C. `aws ec2 check-instance-status`

D. `aws ec2 describe-instance-status`

22. You have been asked to ensure that some of your organization's junior system administrators can access Amazon CloudWatch to look at metrics. They have very limited credentials currently. Which policy can they be given that will enable them to view CloudWatch metrics without granting them additional access to the other AWS services?

A. CloudWatchReadOnlyAccess

B. CloudWatchMetricsAccess

C. MetricsReadOnlyAccess

D. AmazonEC2ReadOnly

23. Your boss has asked you to ensure that your Amazon EC2 instances have metrics being measured every 5 minutes. What type of monitoring should you use?

A. Standard

B. Basic

C. Advanced

D. Detailed

24. Your boss has asked you to ensure that your Amazon EC2 instances have metrics being measured every minute. What type of monitoring should you use?

A. Standard

B. Basic

C. Advanced

D. Detailed

25. You want to be able to store all of your log files from on-premises systems and AWS systems. Which AWS solution will allow you to store all of your log files in one place that will allow Amazon CloudWatch to monitor them?

A. Amazon S3

B. Amazon CloudWatch Events

C. Amazon CloudWatch Logs

D. Amazon EBS

26. You are wanting to move some Solaris servers to AWS from your on-prem datacenter and you would like to take advantage of CloudWatch Logs. Will you be able to install the agent for Linux on your Solaris servers?

A. Yes. All versions of Unix and Linux support the Amazon CloudWatch Logs agent.

B. Yes. Solaris is supported with the Amazon CloudWatch Logs agent.

C. No. Solaris doesn't support Python, which is a requirement of the Amazon CloudWatch Logs agent.

D. No. Solaris isn't supported with the Amazon CloudWatch Logs agent.

27. You want to ensure that you are able to update your Amazon CloudWatch Logs agent on your Red Hat Linux servers without having to manually copy and install the update package. How can you accomplish this task with the least amount of administrative overhead?

A. Use wget to copy the package to the server then run it.

B. Use the Red Hat Package Manager to install awslogs.

C. Copy the package via FTP with an automated file transfer service.

D. You can't update the CloudWatch Logs agent automatically.

28. You have chosen to update an existing server's Amazon CloudWatch agent using the Red Hat Package Manager (RPM). When the agent was first installed, a Python script was used. Since the update through RPM, you are no longer receiving logs in Amazon CloudWatch. When you check the server, you find that the configuration has changed. What is the most likely cause?

A. Configuration issues are caused by updating the agent with Red Hat Package Manager because RPM has technical limitations.

B. The Linux server needs to be restarted for the updated agent installation to take effect and start sending logs to Amazon CloudWatch.

C. Configuration issues are caused by updating the agent with Red Hat Package Manager when it was installed by Python initially.

D. The wrong agent installation package was used; you mistakenly ran the Debian package instead of the RPM package.

29. Which is a type of log that you can get from the Amazon CloudWatch Logs agent for Windows?

A. Firmware log

B. Proprietary logs

C. Website

D. IIS logs

30. Which is a type of log that you can get from the Amazon CloudWatch Logs agent for Windows?

A. Firmware log

B. System logs

C. Website

D. Boot diagnostics logs

31. The Amazon CloudWatch Logs agent for Windows has been installed on an EC2 instance running Windows Server 2016. You look for the EC2Config service but can't find it running. Logs are flowing into Amazon CloudWatch, but why do you not see the EC2Config service as you would on other older servers?

A. EC2Config service is not supported for Windows Server 2016.

B. There is an issue with the CloudWatch Logs Agent for Windows.

C. Your installation of Windows Server 2016 needs to be updated.

D. The CloudWatch Logs Agent didn't actually install; the logs are getting to Amazon CloudWatch another way.

32. You work for a hospital and must ensure that your log data is encrypted at all times. Does Amazon CloudWatch meet this requirement?

A. Yes, but you have to configure it when you install the log agent.

B. No. Log data is only encrypted in transit.

C. Yes. Log data is encrypted at rest and in transit.

D. No. Log data is only encrypted at rest.

33. Your supervisor has asked you if there is a way to create reports with billing data so that they can view billing by usage, or the cost per individual log group. What should you tell your boss?

A. Yes. AWS allows you to get this information with detailed billing.

B. Yes. AWS allows you to get this information with basic billing.

C. No. AWS does not allow you to get this information.

D. No. AWS does not give you the ability to create reports in this way.

34. How many tags can you have in an Amazon CloudWatch log group?

A. 35

B. 50

C. 100

D. 500

35. Your accounting department wants to know if there is a way to identify resources in Amazon CloudWatch so that they can bill back to the individual departments that are utilizing AWS resources. What is the best method you can tell your accounting department to use?

A. Accounting will need to manually track which department needs to get billed for various resources.

B. You can add a prefix to all of the alert names and resource names and Accounting can search on the prefix.

C. Tags can be used for resources and log groups in order to identify which department to bill.

D. There is no way to track which department is using which resources.

36. Your security team has contacted you with concerns regarding the activity of a user in the AWS Management Console. Which service allows you to view all of the activity that was generated under their account?

A. AWS IAM

B. AWS Trusted Advisor

C. Amazon CloudWatch

D. AWS CloudTrail

37. By default, where are AWS CloudTrail trails stored?

A. S3

B. EBS

C. EFS

D. Glacier

38. How do Amazon CloudWatch and AWS CloudTrail work together?

A. Amazon CloudWatch and AWS CloudTrail don't work together at all; they are two separate products.

B. Amazon CloudWatch monitors performance and availability, and AWS CloudTrail feeds API activity into Amazon CloudWatch.

C. Amazon CloudWatch uses AWS CloudTrail to send alerts to end users when a security event occurs.

D. Amazon CloudWatch uses AWS CloudTrail to monitor costs related to alerting and monitoring.

39. Which type of monitoring is free and updates in 5-minute periods in Amazon CloudWatch?

A. Detailed

B. Advanced

C. Basic

D. Simple

40. Which type of monitoring updates in 1-minute periods for an additional charge in Amazon CloudWatch?

A. Detailed

B. Advanced

C. Basic

D. Simple

41. How would you enable Amazon CloudWatch detailed monitoring via the AWS CLI?

A. `aws ec2 monitor-instances --instance-ids <instance-id>`

B. `aws ec2 watch-instances --instance-ids <instance-id>`

C. `aws cloudwatch monitor-instances --instance-ids <instance-id>`

D. `aws cloudwatch watch-instances --instance-ids <instance-id>`

42. How would you disable Amazon CloudWatch detailed monitoring via the AWS CLI?

A. `aws cloudwatch unmonitor-instances --instance-ids <instance-id>`

B. `aws cloudwatch nomonitor-instances --instance-ids <instance-id>`

C. `aws ec2 unmonitor-instances --instance-ids <instance-id>`

D. `aws ec2 nomonitor-instances --instance-ids <instance-id>`

43. Your boss wants to know how many read operations are happening across your Amazon EC2 instances. Which type of statistic will be most useful to give your boss the information they want?

A. Average

B. Maximum

C. Minimum

D. Sum

44. Your boss wants to know the average number of read operations that are happening across your Amazon EC2 instances. Which type of statistic will be most useful to give your boss the information they want?

A. Average

B. Maximum

C. Minimum

D. Sum

45. Your boss wants to know the highest number of read operations that have occurred across your Amazon EC2 instances within a set span of time. Which type of statistic will be most useful to give your boss the information they want?

A. Average

B. Maximum

C. Minimum

D. Sum

46. Your boss wants to know the lowest number of read operations that have occurred across your Amazon EC2 instances within a set span of time. Which type of statistic will be most useful to give your boss the information they want?

A. Average

B. Maximum

C. Minimum

D. Sum

47. Your boss wants to know the total number of read operations metrics that have been gathered from across your Amazon EC2 instances within a set span of time. Which type of statistic will be most useful to give your boss the information they want?

A. SampleCount

B. Sample

C. Number

D. Sum

48. Which steps are necessary to be able to aggregate statistics across multiple instances? (Choose two.)

A. Choose the Amazon EC2 namespace and select Across All Instances.

B. Enable basic monitoring.

C. Choose the Amazon CloudWatch namespace and select Across All Instances.

D. Enable detailed monitoring.

E. Enable standard monitoring.

49. Which are ways that you can choose to filter which statistics you want to view? (Choose three.)

A. By specific trails

B. By specific instance

C. By Auto Scaling group

D. By Elastic Load Balancer

E. By AMI

F. By application load balancer

50. When an alarm is triggered in Amazon CloudWatch, your boss wants the Amazon EC2 instance to self-heal. How can you automatically reboot an Amazon EC2 instance when it is having issues?

A. Set an alarm action to trigger a reboot.

B. Set an alarm action to stop the instance.

C. Set an alarm action to terminate the instance.

D. Set an alarm action to recover the instance.

51. When an alarm is triggered in Amazon CloudWatch that appears to be reporting hardware failure, your boss wants the Amazon EC2 instance to recover itself. How can you recover an Amazon EC2 instance when it is on a host that is having hardware issues?

A. Set an alarm action to trigger a reboot.

B. Set an alarm action to stop the instance.

C. Set an alarm action to terminate the instance.

D. Set an alarm action to recover the instance.

52. Your organization has development workloads that run on Amazon EC2 instances. Your boss has asked you to determine the best method to ensure that the development instances are not left running when they are not in use. What is the best method to accomplish this goal?

A. Use Amazon CloudWatch to watch for low CPU utilization. Set the alarm action to stop the instance when the alarm is triggered.

B. Use Amazon CloudWatch to watch for low CPU utilization. Set the alarm action to terminate the instance when the alarm is triggered.

C. Use Amazon CloudWatch to watch for high CPU utilization. Set the alarm action to stop the instance when the alarm is triggered.

D. Use Amazon CloudWatch to watch for high CPU utilization. Set the alarm action to terminate the instance when the alarm is triggered.

53. When is a good time to use the Terminate alarm action?

A. When an Amazon EC2 instance is currently not needed anymore but will be needed later.

B. When an Amazon EC2 instance needs to be running 24x7.

C. When an Amazon EC2 instance is not needed after finishing a job.

D. You should never use the Terminate alarm action.

54. Your boss would like to view previous Amazon CloudWatch alarms. Where can these be viewed?

A. The Alarms tab in the AWS Management Console

B. The Alarms tab in the Amazon EC2 Management Console.

C. The History tab in the AWS Management Console

D. The History tab in the Amazon CloudWatch Console

55. Your boss has come to you asking if there is an easy way to view the usage each month to see how much their assets in AWS are going to cost. Where can they go to see this information?

A. They can view this information in the AWS Management Console.

B. They can view this information in AWS Billing and Cost Management.

C. They can view this information in AWS Trusted Advisor.

D. They can't; there is no way to monitor for this in AWS.

56. Your security team has asked you if there is a way to report on anyone who made changes in AWS Billing and Cost Management using the root credentials. What should you tell them?

A. No. There isn't a way to tell if a change was made as the root account.

B. No. You can tell that a change was made, but you can't tell who made the change.

C. Yes. You can make a report in Amazon CloudWatch that will tell them if the root user was used to make changes in the AWS Billing and Cost Management Console.

D. Yes. You can make a report in AWS CloudTrail that will tell them if the root user was used to make changes in the AWS Billing and Cost Management Console.

57. Your organization is just getting started using AWS. It has opted to use the AWS Free Tier to do a proof of concept. Your boss wants to ensure that they will get an alert if they will exceed what the AWS Free Tier provides. What is the best way to give them the alert they need with the least amount of administrative overhead?

A. Set up an AWS Free Tier alert in AWS Budgets.

B. Set up an AWS Free Tier alert in Amazon CloudWatch.

C. Set up an AWS Free Tier alert in AWS CloudTrail.

D. Set up a manual billing alert utilizing Amazon CloudWatch.

58. You are the system administrator in charge of getting your organization's AWS environment set up. You want to enable billing alerts, but when you log in with your IAM account, you are unable to do so. Why can't you create the billing alert?

A. Your IAM account doesn't have the necessary permissions; you need more access.

B. You can't set up billing alerts in AWS; you have to arrange them with your technical account manager.

C. You need to be signed in with the AWS account's root user credentials to enable billing alerts.

D. It is not possible to set up billing alerts in AWS.

59. What are the valid statuses you can get from the Amazon EC2 health checks? (Choose two.)

A. Pass

B. Fail

C. OK

D. Impaired

E. Offline

60. You don't like the status checks and the alerting done from the status checks that exist on Amazon EC2. You want to disable the status checks in favor of another solution. How can you disable the Amazon EC2 status checks?

- **A.** You can disable them by turning off the monitoring in the Amazon EC2 instance.
- **B.** You can disable them by installing the Amazon CloudWatch Logs agent and then disabling them through the agent.
- **C.** You can't disable them; they are part of Amazon EC2.
- **D.** You can't disable them; they are part of Amazon EC2. You can disable the alerts that trigger off of the status checks.

61. How can you view the status checks for your organization's Amazon EC2 instances? (Choose two.)

- **A.** Amazon EC2 Console
- **B.** AWS Management Console
- **C.** Command Line
- **D.** Amazon CloudWatch Console
- **E.** AWS CloudTrail Console

62. Where should you create an alarm for a failed Amazon EC2 status check failure?

- **A.** Amazon EC2 Console
- **B.** Amazon CloudWatch Console
- **C.** AWS CloudTrail Console
- **D.** AWS Management Console

63. How long are statistics retained in Amazon CloudWatch?

- **A.** 6 months
- **B.** 12 months
- **C.** 15 months
- **D.** 30 months

64. Which product would you use to monitor all API calls including activities performed on the AWS Management Console against Amazon EC2 and Amazon EBS?

- **A.** Amazon CloudWatch
- **B.** AWS CloudTrail
- **C.** Amazon API Gateway
- **D.** AWS Lambda

65. Where do the trails from AWS CloudTrail store their data?

- **A.** Amazon EBS
- **B.** Amazon EFS
- **C.** Amazon EC2 instance
- **D.** S3 bucket

66. Your boss has asked you if there is a way to validate that all of the AWS services that you rely on are up and operational. What should your answer be?

A. Yes, we can check the Service Health Dashboard.

B. Yes, we can check Amazon CloudWatch.

C. Yes, we can check AWS CloudTrail.

D. No, there is no way to check the AWS services.

67. Your boss has asked you if there is a way to get a personalized view of all the AWS services that you rely on to confirm that they are up and operational. What should your answer be?

A. Yes. We can check the Service Health Dashboard.

B. Yes. We can check AWS CloudTrail.

C. Yes. We can use the Personal Health Dashboard.

D. Yes. We can check Amazon CloudWatch.

68. You log into the Personal Health Dashboard. You see a notification that there is a "Route53 operational issue." You begin getting calls saying that customers aren't able to reach your website. Could these two issues be related?

A. Yes. Amazon Route 53 provides DNS services. If DNS is not working properly, then customers may not be able to reach your resources.

B. Yes. Amazon Route 53 provides caching services. If it can't cache content, then customers may not be able to reach your resources.

C. No. Amazon Route 53 errors wouldn't show up in the Personal Health Dashboard.

D. No, the issues couldn't be related.

69. Your boss has approached you about giving access to only a specific set of Amazon EC2 instances in Amazon CloudWatch. How would you accomplish this in AWS IAM?

A. You specify which Amazon EC2 instances can be accessed in an AWS IAM policy.

B. You give permissions to the individual Amazon EC2 instances, and those permissions will carry over into Amazon CloudWatch.

C. You can't grant access in Amazon CloudWatch for specific resources with AWS IAM.

D. You can create a role that will define granular permissions for individual Amazon EC2 instances in Amazon CloudWatch.

70. You have been tasked by your boss to ensure that you receive alerts when a particular event ID occurs on both your on-premises systems and your Amazon EC2 instances. Which product would allow you to collect the logs in a single place, filter on the event ID, and send an alert?

A. AWS CloudTrail

B. Amazon CloudWatch Logs

C. Amazon EC2 Logs

D. Amazon SNS

71. Your boss wants to leverage your existing investment in AWS as much as possible and has asked you to implement a real-time performance and availability monitoring solution that will cover both your on-premises systems and your resources in the AWS cloud. What should you suggest?

A. A third-party tool like SolarWinds

B. AWS CloudTrail

C. Amazon SNS

D. Amazon CloudWatch Logs

72. You have strict regulatory requirements on log retention. You need to find a solution that will allow you to collect logs and store them at a lower cost. What would be the best solution to meet this need?

A. Amazon SNS

B. AWS CloudTrail

C. Amazon CloudWatch Logs

D. Amazon EBS

73. Your security team has mandated that you need to avoid using service accounts unless absolutely necessary because of the overhead in managing password rotation. You want to deploy the Amazon CloudWatch Logs agent. What could you use to authenticate the agent that is not a service account?

A. Access keys

B. AWS IAM

C. Active Directory

D. There isn't any option other than a service account.

74. Your security team has mandated that you need to avoid using service accounts unless absolutely necessary because of the overhead in managing password rotation. You want to deploy the Amazon CloudWatch Logs agent. What could you use to authenticate the agent that is not a service account?

A. Active Directory

B. AWS IAM

C. IAM roles

D. There isn't any option other than a service account.

75. Your operations center has asked if there is a better way to analyze and visualize the data that has been made available to them with Amazon CloudWatch. What would you recommend?

A. Amazon CloudWatch Logs agent

B. AWS CloudTrail

C. Amazon Redshift

D. Amazon CloudWatch Logs Insights

76. Your security team wants to minimize the amount of metrics that are kept in Amazon CloudWatch. They have asked you to delete the older metrics. How will you accomplish this?

A. You can't delete metrics; they are retained for the life of the account.

B. You can't delete metrics, though metrics do expire according to a schedule.

C. Log into the AWS Management Console with your IAM account and delete the metrics.

D. Log into the AWS Management Console with the root account and delete the metrics.

77. You have an application that you need to monitor. As it is critical to the business, you have been asked if you can create a metric that can record data every second. You also need to be able to retrieve it every second. How can you accomplish this?

A. Create a custom metric with a fast resolution.

B. Create a custom metric with a standard resolution.

C. Create a custom metric with a high resolution.

D. Create a custom metric with a detailed resolution.

78. Your boss has asked you if you can get pre-built metrics at a 1-second sampling rate as you can with your custom metrics. What should your response be?

A. Yes, you can use high resolution on pre-built metrics.

B. Yes, you can use high resolution on all metrics.

C. Yes, you can use standard resolution on all metrics.

D. No, you can't use high resolution for pre-built metrics.

79. How would you set a custom metric to use high resolution?

A. Set MetricResolution to 1 using the PutMetricRequest API.

B. Set StorageRetention to 1 using the PutMetricRequest API.

C. Set StorageResolution to 1 using the PutMetricRequest API.

D. Set MetricRetention to 1 using the PutMetricRequest API.

80. Your boss wants to use high-resolution metrics because they want to be able to get data every 15 seconds. They are concerned about additional cost from using high-resolution metrics. What should you tell your boss?

A. High-resolution metrics are more expensive.

B. High-resolution metrics are less expensive.

C. High-resolution metrics cost the same as standard.

D. You can't do 15-second periods with high resolution.

81. You have installed the Amazon CloudWatch Logs agent on a set of Amazon EC2 systems. They are sending logs to Amazon CloudWatch every 5 seconds, but you would prefer that happened every 15 seconds instead. What can you do?

A. Adjust the Amazon CloudWatch Logs agent to send logs every 15 seconds.

B. You can't adjust the 5-second time; it is the default setting.

C. Set Amazon CloudWatch to pull the data every 15 seconds.

D. Set AWS CloudTrail to pull the logs every 15 seconds.

82. You have begun sending system logs into Amazon CloudWatch. You want to ensure that you see any logs that contain the word *error* in them. How would you achieve this?

A. Statistic filters

B. Log filters

C. Metric filters

D. Error filter

83. You work for a financial institution and you need to parse your log data for account numbers. You have a regex query built that has been used in other solutions. How can you parse your log data for the regex that will find account numbers?

A. Amazon CloudWatch Metric Filters

B. AWS Management Console

C. Amazon CloudWatch

D. Amazon Kinesis

84. You have created some high-resolution custom metrics and want to ensure that Amazon CloudWatch will trigger an alarm no more than 10 seconds after an incident occurs. How can this be accomplished?

A. Create a high-resolution Amazon CloudWatch alarm.

B. Create a standard Amazon CloudWatch alarm.

C. Create a detailed Amazon CloudWatch alarm.

D. You can't set an Amazon CloudWatch alarm for under a minute.

85. You have created an Amazon CloudWatch alarm for your Amazon EC2 instances and it is constantly in the ALARM state. None of your systems are having any issues. How can you resolve the issue?

A. Delete the alarm and then re-create it.

B. Adjust the threshold that the alarm is set to so that it is no longer breached.

C. Reboot the Amazon EC2 instances.

D. Install the Amazon CloudWatch Logs agent.

86. Your Operations Center would like to create a dashboard to track Amazon CloudWatch alarms. What would be the best solution?

A. Amazon CloudWatch Logs

B. AWS CloudTrail

C. Amazon EC2 with business analytics software

D. Amazon CloudWatch Dashboards

87. You want to view how well your systems and resources in AWS are doing at any point in time. You have systems in multiple regions. How do you get a dashboard-like experience for your availability and performance data?

A. You can't set up a dashboard that can monitor across all regions.

B. Use Amazon CloudWatch Dashboards.

C. Use Amazon CloudWatch Logs.

D. Use an Amazon CloudWatch Logs agent.

88. Your security team has asked you to ensure that API calls are being logged. You know that you can use AWS CloudTrail to accomplish this. What do you need to do next?

A. AWS CloudTrail is enabled, but you need to tell it what type of API calls to log.

B. AWS CloudTrail is enabled, but you need to configure a trail to start logging API calls.

C. Nothing; AWS CloudTrail is enabled and configured by default.

D. You need to enable AWS CloudTrail to begin recording API calls.

89. Your security team has asked you to ensure that *all* API calls are being logged. You know that you can use AWS CloudTrail to accomplish this. What do you need to do next?

A. AWS CloudTrail is enabled, but you need to tell it what type of API calls to log.

B. AWS CloudTrail is enabled, but you need to configure a trail to start logging all API calls.

C. Nothing; AWS CloudTrail is enabled and configured by default.

D. You need to enable AWS CloudTrail to begin recording API calls.

90. Your security team wants to ensure that all activity within the AWS Management Console is recorded. What is the best solution that meets this goal?

A. AWS Trusted Advisor

B. Amazon CloudWatch Logs

C. AWS CloudTrail

D. Amazon CloudWatch

91. You are the system administrator for a rapidly growing company. While you only have resources in one region currently, you know that you will expand into other regions soon. How can you ensure that API calls are captured automatically for any new regions that are added? (Choose two.)

A. Select Global from the region drop-down, then create the trail.

B. Select the existing region in the trail configuration page.

C. Select Yes to apply to all regions in the trail configuration page.

D. In the CLI, you set the parameter IsMultiRegionTrail to True.

E. You can't automatically add new regions to an AWS CloudTrail trail.

92. Your boss wants you to create two separate trails in Amazon CloudWatch, one for management and one for data. Can you create the trails in the way that your boss wants you to?

A. Yes, you can create two separate trails and separate management activity from data activity.

B. No, you can't put management and data traffic into separate trails or create multiple trails.

C. No, you can't put management and data traffic into separate trails, though you can create multiple trails.

D. No, you can't create multiple trails, though you can separate management and data activity.

93. Your security team has required that you encrypt your AWS CloudTrail log files. What do you need to do to ensure that they are encrypted and only accessible to those who need to review them?

A. Nothing; you can't encrypt AWS CloudTrail log files.

B. Nothing; they are encrypted with S3 SSE by default.

C. They are encrypted by default using S3 SSE; you can use S3 bucket policies or IAM to control access.

D. You need to enable encryption in S3 so that the AWS CloudTrail log files are encrypted.

94. Your security team has made the requirement that controls need to be implemented to prevent accidental deletion of AWS CloudTrail log files. What is the best solution for this?

A. Restrict access to the S3 bucket.

B. Enable MFA Delete.

C. Enable versioning.

D. Use lifecycle policies to archive deleted objects.

95. Your legal team has asked you to ensure that AWS CloudTrail log files are only retained for 90 days. What can you do to meet their needs?

A. You can't adjust the retention time frame on AWS CloudTrail log files.

B. You make the change in AWS CloudTrail to reflect the 90-day rule.

C. You make the change in Amazon CloudWatch to reflect the 90-day rule.

D. You make a lifecycle rule in S3 to delete log files older than 90 days.

96. Your developers are checking an AWS CloudTrail log file troubleshooting their work. They are complaining that API calls they are making are not showing up until 15 minutes later. What can you do to remediate this issue?

A. The AWS CloudTrail trail is not configured properly; you need to reconfigure it to log items faster.

B. There is nothing to remediate; AWS CloudTrail log files typically get an event around 15 minutes after the API call.

C. You should change the timing between the delivery of the event and the occurrence of the event to 5 minutes.

D. You should change the timing between the delivery of the event and it occurring to 1 minute.

97. You look in your S3 bucket where AWS CloudTrail stores its log files and you notice that there are no log files during the late evening hours. What is the most likely cause for the missing log files?

A. There was no API activity during this time frame.

B. There was a misconfiguration in AWS CloudTrail.

C. You don't have permissions to view the log files.

D. AWS CloudTrail doesn't have the access it needs to write the log files.

98. Your security team has asked for you to provide a way to validate that AWS CloudTrail log files have not been modified since being placed in the S3 bucket. What can you do to prove that the files have not been changed with the least amount of administrative effort?

A. Enable encryption in Amazon S3.

B. Create an AWS Lambda function to check the hashes every hour and compare against a database of the original hashes.

C. Enable AWS CloudTrail log file integrity validation.

D. Manually hash the files and check against known hashes.

99. Your security team wants to ensure that AWS resources are built according to the organizational standards that have been set. How can you prove to your security team that your systems are using the desired configurations?

A. Use Amazon CloudWatch.

B. Use AWS CloudTrail.

C. Use AWS Config.

D. Use AWS Lambda.

100. Your legal department wants to know anytime a configuration change is made on one of their systems. They want to receive a notification when the change is made. How can you ensure that the legal department is aware of any changes made to their server?

- **A.** Enable Amazon CloudWatch and create an SNS topic; subscribe them to the topic.
- **B.** Enable AWS CloudTrail and create an SNS topic; subscribe them to the topic.
- **C.** Enable AWS Config and create an SNS topic; subscribe them to the topic.
- **D.** Enable AWS Config and create an SMS topic; subscribe them to the topic.

101. One of your critical applications just suffered an outage. It is suspected that a change caused the outage but there is no scheduled change in your change management calendar. How can you figure out who made the change and what the change was?

- **A.** Use Amazon CloudWatch to check for events that happened around the time of the outage.
- **B.** Use AWS CloudTrail to look at any of the API calls made around the time that it is believed the change occurred to see who made the change and what the change was.
- **C.** Setup AWS Config to send a message to an SNS topic when any config changes are made.
- **D.** Use AWS Config to view the configuration history of the resource that suffered the outage and AWS CloudTrail to see who made the change.

102. You are the system administrator in charge of your organization's AWS resources. You work for a hospital and have been asked by the internal audit team for a report that proves that you have implemented the proper controls to maintain HIPAA compliance. How can you do this within AWS?

- **A.** Create rules that evaluate your systems for the desired controls in AWS Config.
- **B.** Use AWS CloudTrail to check for inappropriate API calls.
- **C.** Use Amazon CloudWatch to monitor for compliance.
- **D.** There is no automated tool; you must do it all manually.

103. You are the system administrator for your organization in charge of its AWS infrastructure. You have configured the desired configurations for your systems. You want to ensure that systems are never out of compliance. Can you prevent users from making changes with AWS Config?

- **A.** Yes, select the Enforce option when you set up AWS Config.
- **B.** Yes, it does it automatically without any further interaction.
- **C.** No, AWS Config is only able to monitor configurations, not change them.
- **D.** No, AWS Config doesn't monitor configuration drift.

104. You have multiple accounts under AWS Organizations. You want to combine the results of AWS Config under AWS Organizations. How can you do this?

- **A.** Create an aggregator in one of the regions that you want to monitor.
- **B.** Create an aggregator in AWS Organizations.

C. You can't view the AWS Config data from multiple regions, though you can view it for multiple regions.

D. You can't view the AWS Config data from multiple regions or accounts in one area.

105. You have multiple accounts under AWS Organizations. You want to combine the results of AWS Config under one of the regions that most of your resources reside in. How can you do this?

A. Create an aggregator in one of the regions that you want to monitor.

B. Create an aggregator in AWS Organizations.

C. You can't view the AWS Config data from multiple regions, though you can view it for multiple regions.

D. You can't view the AWS Config data from multiple regions or accounts in one area.

106. You want to ensure that AWS Config is enabled for all three regions that your organization is using. How would you enable AWS Config for all three regions?

A. It is automatically enabled for all regions.

B. You need to enable it once for all regions.

C. You need to enable it once per region.

D. You can't use AWS Config for that many regions.

107. Your security team has asked you to make sure that any changes to the desired configurations in AWS Config are monitored so that they know who made the change. Which product can be used to achieve this request?

A. AWS Config

B. Amazon CloudWatch

C. AWS CloudTrail

D. AWS IAM

108. You currently have 145 individual AWS Config rules built for your organization's environment. You need to make 10 more rules for new criteria that your legal team wants you to monitor for. Will you be able to create 10 more rules?

A. Yes, you can create unlimited rules.

B. Yes, but you will need to request an increase on the limit from AWS.

C. No, because you can't have more than 150 rules.

D. No, because you can't add more rules.

109. Your boss wants you to set up a periodic rule in AWS Config, and they want it to run every 6 hours. How should you respond to this request?

A. Set up the periodic rule for 3 hours because you can't set it to 6.

B. Set up the periodic rule to run every 6 hours.

C. Set up the periodic rule to run every 12 hours because you can't set it to 6.

D. Tell your boss that AWS Config can only do change-triggered rules.

110. You are not using AWS Organizations, but you want to aggregate your AWS Config data from all of your other accounts. Besides setting up AWS Config and the aggregator, what else do you need to do?

A. There is nothing else to set up; once the aggregator is created it will work.

B. Create a role and assign it to the aggregator account.

C. Add an AWS IAM account for the aggregator to use in each individual AWS account.

D. Authorize the aggregator account in each individual AWS account.

111. A resource has been reported as noncompliant by AWS Config and a notification has been sent. When the rules are run again, the resource is still noncompliant, but you didn't get a notification. Why is this?

A. AWS Config is having a service outage.

B. AWS Config is misconfigured so it is not sending messages properly.

C. This behavior is by design; notifications are sent when the status changes.

D. You will only get one notification when it fails.

112. You have AWS Config configured in your AWS account. You have added a security group to an Amazon EC2 instance. Which resources will have changes recorded in AWS Config?

A. Amazon EC2 instance

B. The security group

C. Primary resource and related resources

D. All of these

113. Your Operations Center team would like to know what kinds of things AWS Config can record. What should you include in your response?

A. All of the following options

B. OS patches

C. Application installations

D. Network configurations

114. Which account is used in AWS Organizations to create an organization, invite new AWS accounts, and remove AWS accounts?

A. root

B. master

C. An IAM user with sufficient access

D. A shared access key

115. You have a new person in Accounting who is in charge of paying for your AWS account charges. They have asked you if there is a way to see what the charges are so far. Where should you tell them to go?

A. AWS Budgets

B. AWS Management Console

C. AWS Billing and Cost Management Dashboard

D. AWS Trusted Advisor

116. You have been asked by your manager to create a report that will forecast how much AWS is going to cost your organization over the next three months. You have been using AWS for six months. Which tool will provide this information?

A. AWS Organizations

B. AWS Trusted Advisor

C. AWS Budgets

D. Cost Explorer

117. Your accounting department likes the view that the Billing and Cost Management Dashboard gives them, but they don't want to have to go to each individual AWS account to view billing for the entire organization. What should you implement to allow them to view billing for the entire organization?

A. AWS Trusted Advisor

B. AWS Organizations

C. AWS Management Console

D. AWS Budgets

118. Your boss wants to view the current amount due on your AWS account. Where should you tell your boss to look?

A. AWS Management Console

B. AWS Trusted Advisor

C. AWS Budgets

D. AWS Cost Explorer

119. Your boss wants to view the forecasted amount due on your AWS account. Where should you tell your boss to look?

A. AWS Cost Explorer

B. AWS Trusted Advisor

C. AWS Management Console

D. AWS Budgets

120. Your accounting department wants to know if there are ways to save on costs for EC2 instances. When they view the Reservation Recommendations screen in AWS Cost Explorer, they get a message saying that there are no recommendations available at this time. What is a possible cause of this error?

A. You are using instance types that can't be set as reserved instances.

B. Your instances haven't run long enough to generate recommendations.

C. They don't have permissions to view cost and budget items.

D. You are using instance sizes that can't be used with reserved instances.

121. Which services does AWS Trusted Advisor not provide?

A. Cost savings recommendations

B. Performance recommendations

C. Security recommendations

D. Alarms for going over budget

122. You want to use AWS Trusted Advisor to monitor how well you are setting things up in your organization's AWS account. When you log in, you are disappointed to see only seven checks. How can you get access to all of the checks within AWS Trusted Advisor? (Choose two.)

A. Upgrade to Developer-level support.

B. Upgrade to Enterprise-level support.

C. Upgrade to Teams-level support.

D. You can't upgrade; there are only seven checks.

E. Upgrade to Business-level support.

123. Which of the following is a category that AWS Trusted Advisor checks?

A. Security

B. Cost monitoring

C. Budgeting

D. System vulnerabilities

124. Which of the following is a category that AWS Trusted Advisor checks?

A. Network intrusions

B. Application configurations

C. Service limits

D. Conflicting security groups and NACLs

125. Which of the following is a category that AWS Trusted Advisor checks?

A. Vulnerability scanning

B. Budgeting

C. Cost reporting

D. Performance

126. Which of the following is a category that AWS Trusted Advisor checks?

A. Network intrusions

B. Cost optimization

C. Security scans

D. Cost budgeting

127. Which of the following is a category that AWS Trusted Advisor checks?

A. IOPS optimization

B. Budgeting

C. Fault tolerance

D. Available IP space

128. Trusted Advisor continuously alerts on one of your resources and your boss has asked you to ensure that AWS Trusted Advisor no longer alerts on that resource. How can you accomplish this?

A. Add an exclusion for reporting the resource at the resource level.

B. Add an exclusion for reporting the resource at the check level.

C. Add an exclusion for reporting the resource in Amazon CloudWatch.

D. There is no way to disable the alerts from occurring in AWS Trusted Advisor.

129. You have remediated an issue that was being reported by AWS Trusted Advisor. You have hit refresh multiple times in the past minute but nothing has changed. What is the most likely cause?

A. You did not properly remediate the issue that AWS Trusted Advisor was reporting.

B. You have to wait for 15 minutes to refresh a check from the last time it was checked.

C. You have to wait for 10 minutes to refresh a check from the last time it was checked.

D. You have to wait for 5 minutes to refresh a check from the last time it was checked.

130. You try to create an elastic IP address and you get a message that states that your service limit has been reached. Where can you go to verify that this is the case?

A. Amazon CloudWatch

B. AWS Trusted Advisor

C. AWS CloudTrail

D. AWS Config

131. You try to create an elastic IP address and you get a message that states that your service limit has been reached. You have verified in AWS Trusted Advisor that the service limit has indeed been reached. How can you resolve the issue? (Choose two.)

A. Increase your service limits from the AWS Management Console.

B. Increase your service limits from the AWS CLI.

C. Contact AWS to request a service limit increase.

D. Deprovision old resources to free up unused elastic IP addresses.

E. Increase your service limits from the AWS SDK.

132. Your organization's accounting department is looking at reservation recommendations but is not seeing any. You use spot instances to support batch jobs that can be easily interrupted. How can you explain to your accounting department why they are not seeing any recommendations?

A. AWS Trusted Advisor uses on-demand rates to calculate savings with reserved instances.

B. Spot instances aren't up long enough to generate recommendations in AWS Trusted Advisor.

C. Spot instances don't show up in AWS Trusted Advisor.

D. The accounting department doesn't have permissions to view the reserved instance recommendations.

133. Your security department wants an easy way to monitor the overall security posture of your AWS environment. Which tool should you recommend to them?

A. AWS WAF

B. AWS Systems Manager

C. Amazon Inspector

D. Amazon GuardDuty

134. Your security department wants to know which processes are running on open ports. How can you give them this information? (Choose two.)

A. Run a scan from Amazon Inspector.

B. Run a scan with Amazon GuardDuty.

C. Use AWS WAF.

D. Install the Amazon Inspector agent.

135. Your security department has asked you for a report that includes how well your systems are lining up with CIS benchmarks. How can you provide them with this report?

A. Use Amazon Inspector to run an assessment template that contain the CIS rules package desired.

B. Use AWS Config to run an assessment template that contains the CIS rules package desired.

C. Use AWS Systems Manager to run an assessment template that contains the CIS rules package desired.

D. You can't; there isn't a report like this.

136. You have just begun using Amazon Inspector to analyze your systems. You get a call stating that Amazon Inspector is causing performance impacts; however, you do not have the agent installed, and you don't currently have an assessment running. What should your response be?

A. Amazon Inspector couldn't be the cause since you are not currently scanning the environment.

B. Amazon Inspector is probably the issue because the agentless configuration is known to cause performance impacts.

C. Amazon Inspector is not likely to be the cause of the performance issue as the agentless configuration is not supposed to cause performance issues.

D. Amazon Inspector is the cause of the performance issue as the agentless configuration has been known to cause performance issues.

137. You have been asked to create your own rules packages for Amazon Inspector assessment templates to use. How do you create a rules package?

A. You can't create rules packages.

B. Create the rules package inside of the Amazon Inspector Dashboard.

C. Create the rules package inside of the AWS Config Dashboard.

D. Create the rules package inside of the AWS Systems Manager Dashboard.

138. You have been asked to scan your application servers for a vulnerable version of software. The software was installed using Ansible. When you look at the scan, you don't see the application listed. What is the most likely cause?

A. Ansible is not supported for use in AWS.

B. Amazon Inspector can only find applications installed by the operating system's package manager.

C. The application is not supported in Amazon Inspector.

D. Amazon Inspector can't tell you application version numbers.

139. You have been asked to provide a basic report based on the findings of Amazon Inspector for the executives of your organization. What type of report should you run from Amazon Inspector?

A. Full report

B. Executive report

C. Findings report

D. Basic report

140. You have been asked to provide a detailed report based on the findings of Amazon Inspector for the members of the security team in your organization. What type of report should you run from Amazon Inspector?

A. Full report

B. Executive report

C. Findings report

D. Basic report

141. Your security team has come to you and asked if AWS has a solution that will allow them to monitor network traffic for threats. How should you respond?

A. Yes, Amazon GuardDuty.

B. Yes, Amazon Inspector.

C. Yes, but it's only available via a third party.

D. No, there is no built-in way to do this.

142. Which AWS service identifies threats throughout your AWS account by analyzing VPC Flow Logs, DNS logs, and CloudTrail events?

A. Amazon CloudWatch

B. Amazon Inspector

C. Amazon GuardDuty

D. Amazon Macie

143. Which AWS services classifies data in S3 and catalogs the normal behaviors from users who are accessing that data?

A. Amazon CloudWatch

B. Amazon Inspector

C. Amazon GuardDuty

D. Amazon Macie

144. Which of these is not something that Amazon GuardDuty monitors for?

A. Instance compromise

B. Account compromise

C. Reconnaissance activity

D. DDoS

145. Your security team wants to be notified when Amazon GuardDuty finds a threat on the network. Which products can be used with Amazon GuardDuty to send them alerts? (Choose two.)

A. Amazon CloudWatch Logs

B. Amazon CloudWatch Events

C. Amazon SNS

D. Amazon SQS

E. Amazon Inspector

146. You have been asked by your organization's CISO how long Amazon GuardDuty will retain the findings that it has alerted on as your organizational standard is 90 days. What should you tell the CISO?

A. 90 days

B. 180 days

C. 45 days

D. 30 days

147. You have a lot of sensitive data in your S3 buckets and you have been asked if there is a solution to classify sensitive data and then monitor it for usage. Which product would fit the criteria?

A. Amazon Inspector

B. Amazon Macie

C. Third-party product

D. There is no product that will meet these requirements.

148. You want to see how well your environment compares to the five pillars of the Well-Architected Framework. Which tool could you use to get a report regarding how well your workloads fit into the AWS Well-Architected Framework?

A. AWS Well-Architected Tool

B. Amazon CloudWatch

C. AWS CloudTrail

D. Amazon Inspector

149. You want to be able to monitor what software is installed and add licenses to installed software across your on-prem systems and your AWS systems. Which products will allow you to do this? (Choose two.)

A. Amazon Inspector

B. AWS Systems Manager

C. AWS License Manager

D. AWS Config

E. Amazon CloudWatch

150. You are using AWS License Manager to monitor license usage in your account. You want to be able to manage licensing in all of the AWS accounts in your organization. What is the most efficient way to manage your licenses?

A. Have your IAM account added to each AWS account.

B. Set up the AWS accounts in AWS Organizations.

C. Have individual account owners report license usage.

D. You can't centrally manage your license for all AWS accounts.

151. Which of these is a use case for Amazon CloudWatch?

A. Infrastructure automation and orchestration

B. Infrastructure security and privacy

C. Infrastructure patching and updates

D. Infrastructure monitoring and troubleshooting

152. Which of these is a use case for Amazon CloudWatch?

A. Resource management

B. Resource optimization

C. Resource allocation

D. Resource security

153. Which of these is a use case for Amazon CloudWatch?

A. Application load balancing

B. Application routing

C. Application monitoring

D. Application geolocation

154. Which of these is a use case for Amazon CloudWatch?

A. Log storage

B. Log retention

C. Log rotation

D. Log analytics

155. Your boss wants to be able to search for specific data from an event field and have those queries appear on an Amazon CloudWatch Dashboard. Since you have queries built in regex already, how would you use the regex queries to search for the data from an event field?

A. Amazon CloudWatch Logs Insights

B. Amazon Kinesis

C. Amazon Athena

D. Amazon RedShift

156. Which product allows you to take Amazon CloudWatch logs and use interactive queries and visualizations with the data in addition to creating Amazon CloudWatch Dashboards?

A. Amazon CloudWatch Logs

B. Amazon CloudWatch Events

C. Amazon CloudWatch Logs Insights

D. Amazon CloudWatch

157. Which open-source solutions are popular for gathering custom application metrics for Amazon CloudWatch?

A. REST

B. Solarwinds

C. collectd

D. dmesg

E. StatsD

158. Your monitoring team has asked you if there is a way to integrate Amazon CloudWatch graphs into their existing solution so that they can see on-prem and AWS systems from the same source. What should you tell them to use?

A. Amazon CloudWatch Logs

B. Amazon CloudWatch Logs agent

C. Amazon CloudWatch snapshot graphs

D. Amazon CloudWatch APIs

159. What is a common use case for AWS CloudTrail?

A. Firewalling

B. Compliance aid

C. API management

D. Monitoring logs

160. What is a common use case for AWS CloudTrail?

A. Monitoring logs

B. Detecting application issues

C. Detecting data exfiltration

D. Detecting HTTP response codes

161. What is a common use case for AWS CloudTrail?

A. Installing software

B. Installing patches

C. Monitoring for installed software

D. Security analysis

162. What is a common use case for AWS CloudTrail?

A. Operational issue troubleshooting

B. Installing security updates

C. Monitoring logs

D. Monitoring for HTTP response codes

163. Which data event type in AWS CloudTrail allows you to see when an AWS Lambda function was executed and who executed it?

A. Invoke API

B. Management events

C. AWS Lambda logs

D. Log

164. For regulatory purposes, you need to ensure that AWS CloudTrail trail data is stored for one year with easy access, and then you want the trail data to be deleted. Which solution provides the correct response with the least amount of administrative effort?

A. Save trails to S3 and manually delete data after one year.

B. Save trails to S3 and create a script that runs daily and deletes trails older than one year.

C. Save trails to S3 and use lifecycle policies to delete trails older than one year.

D. There is no way to accommodate this request in AWS.

165. Name one of the benefits of using AWS Systems Manager?

- **A.** Monitoring logs
- **B.** Monitoring API calls
- **C.** Monitoring vulnerabilities in your environment
- **D.** Detecting problems more quickly

166. Name one of the benefits of using AWS Systems Manager?

- **A.** API Management
- **B.** Automation
- **C.** Federated access
- **D.** Log monitoring

167. Name one of the benefits of using AWS Systems Manager?

- **A.** Improve network accessibility
- **B.** Improve visibility and control
- **C.** Improve security assessments
- **D.** Improve API management

168. Name one of the benefits of using AWS Systems Manager?

- **A.** Manages hybrid cloud environments
- **B.** Improves visibility into logs
- **C.** Makes security assessments more accessible
- **D.** Provides visibility into API calls

169. Name one of the benefits of using AWS Systems Manager?

- **A.** Manage API calls
- **B.** Perform security assessments
- **C.** Maintain security and compliance
- **D.** Monitor logs

170. What is the benefit of the Run Command in AWS Systems Manager?

- **A.** Provides console access to the system without the need for remote access ports to be open
- **B.** Provides console access to Linux hosts via SSH
- **C.** Provides automation of tasks so long as remote access ports are open
- **D.** Provides automation of tasks without the need for remote access

171. What is the benefit of the Session Manager in AWS Systems Manager?

- **A.** Allows remote console sessions via an interactive web browser with no need to open inbound ports
- **B.** Allows remote console sessions via an interactive web browser once the necessary ports are open

C. Allows configuration management and tracking

D. Allows management of APIs

172. What is the benefit of the Patch Manager in AWS Systems Manager?

A. Patch management and reporting for Windows systems only

B. Patch management and reporting for Linux systems only

C. Patch management and reporting for AWS systems only

D. Patch management and reporting for on-prem and AWS systems

173. What is the benefit of the State Manager in AWS Systems Manager?

A. Backs up system state for on-prem and AWS resources

B. Backs up system state for AWS resources only

C. Provides configuration management for on-prem and AWS resources

D. Provides configuration management for AWS resources only

174. What is the benefit of the Parameter Store in AWS Systems Manager?

A. Centralized storage of license keys, database stings, and secrets

B. Used only to store secrets for AWS KMS

C. Used only to store secrets for AWS IAM

D. Used only to store parameters for AWS Lambda

175. Your boss would like to have a single "source of truth" to run queries against the data from the AWS services you use. Is there a way to accomplish this within AWS?

A. Yes, you can query data from the other AWS services with Amazon CloudWatch.

B. Yes, you can query data from the other AWS services with Amazon Athena.

C. Yes, you can query data from the other AWS services with AWS CloudTrail.

D. No, there is not a way to accomplish this in AWS.

176. Which AWS product allows you to analyze the data within Amazon S3 and run queries against it?

A. Amazon CloudFront

B. Amazon RDS

C. Amazon Athena

D. AWS Lambda

177. Your boss wants to be able to not only analyze the data from the various services you use in AWS but also visualize that data. Which two services will allow you to analyze the data from the AWS services and visualize the data as well? (Choose two.)

A. Amazon Athena

B. Amazon QuickSight

C. AWS CloudTrail

D. AWS Lambda

E. Amazon Inspector

178. You need a location where you can store persistent metadata related to Amazon S3. Which AWS service will allow you to accomplish this task?

A. Amazon Athena

B. AWS Glue Data Catalog

C. Amazon RDS

D. Amazon Elasticache

179. Your boss wants to be able to use visualizations within Amazon QuickSight, and to be able to use Active Directory security groups with the least amount of administrative effort. You are using AWS Directory Service already. Which edition of Amazon QuickSight should you choose?

A. Developer

B. Standard

C. Basic

D. Enterprise

180. How is Amazon QuickSight billed?

A. Pay-per-session

B. Pay-per-transaction

C. Pay-per-minute

D. Pay-per-hour

181. What is one of the benefits of Amazon Athena?

A. Amazon Athena is available for a flat monthly rate.

B. Amazon Athena is free.

C. Amazon Athena is a serverless solution.

D. Amazon Athena only requires one server.

182. What is one of the benefits of Amazon Athena?

A. Supports standard SQL

B. Supports proprietary SQL

C. Uses EBS as its data store

D. Needs input to be in JSON or CSV

183. How is Amazon Athena billed?

A. Per session

B. Per transaction

C. Per query, $1/TB scanned

D. Per query, $5/TB scanned

184. What is one of the benefits of Amazon Athena?

A. Uses SQS to queue queries

B. Uses parallel query execution

C. Uses Elasticache to speed up query execution

D. Uses DynamoDB to speed up query execution

185. What is a common use case for AWS Config?

A. Security assessments

B. Continuous monitoring of API calls

C. Continuous monitoring of logs

D. Continuous monitoring of configuration changes

186. What is a common use case for AWS Config?

A. Help troubleshoot issues related to configuration changes.

B. Help troubleshoot issues related to permissions.

C. Help troubleshoot issues related to storage space.

D. Help troubleshoot issues related to processor usage.

187. What is a common use case for AWS Config?

A. Audit configurations for vulnerabilities.

B. Audit configurations for compliance with organizational baselines.

C. Audit configurations for best practices.

D. Audit configurations for bad AMI IDs.

188. What is a common use case for AWS Config?

A. View compliance status of API calls made in the environment.

B. View compliance status of services based on logs.

C. View compliance status for configurations across multiple AWS accounts.

D. View compliance status of password policy in AWS IAM.

189. What is a common use case for AWS Config?

A. Improve change management capabilities and tracking.

B. Improve security assessment capabilities.

C. Improve monitoring of logs.

D. Improve monitoring of APIs.

190. What is a common use case for Amazon Inspector?

A. Identify exploits on the network.

B. Identifying vulnerabilities in applications

C. Identifying best practices according to the Well-Architected Framework

D. Identifying configuration changes in your environment

191. What is a common use case for Amazon Inspector?

- **A.** Assess configurations for changes to your environment.
- **B.** Assess the API calls in your environment for API usage that is not secure.
- **C.** Alert you to a misconfiguration on a NACL that would prevent outbound traffic.
- **D.** Assess your AWS environment against security best practices.

192. What is a common use case for Amazon Inspector?

- **A.** Identify attack traffic on the network.
- **B.** Monitor API calls being used in your environment.
- **C.** Perform assessments within the CI/CD pipeline.
- **D.** Identify configuration changes that have occurred.

193. What is a common use case for Amazon Inspector?

- **A.** Validate security best practices during application development.
- **B.** Validate that current patch levels are correct and patch if they are not.
- **C.** Validate that user access for AWS services is appropriate.
- **D.** Validate that configurations meet your organization's baselines.

194. What is a common use case for Amazon Inspector?

- **A.** Support development shops that use Waterfall methodology.
- **B.** Support development shops that use Agile methodology.
- **C.** Monitor API calls for insecure requests.
- **D.** Monitor for unauthorized configuration changes.

195. What is a common use case for Amazon Inspector?

- **A.** Patch machines that are not on the current patch level.
- **B.** Monitor your network for intrusions.
- **C.** Define the standards or best practices that your applications must adhere to.
- **D.** Compare best practices of the Well-Architected Framework to the current state.

196. Which of these responses is a benefit of Amazon GuardDuty?

- **A.** Compare the environment to the best practices laid out in the Well-Architected Framework.
- **B.** Perform security assessments.
- **C.** Identify threats on the network.
- **D.** Maintain patch levels for systems.

197. Which of these responses is a benefit of Amazon GuardDuty?

- **A.** Automated responses to identified threats
- **B.** Identification of stale user accounts
- **C.** Identification of users/groups with excessive permissions
- **D.** Automated security assessments

198. Which of these responses is a benefit of Amazon GuardDuty?

A. Maintain desired patch levels.

B. Manage encryption keys for your AWS environment.

C. Support a single AWS account.

D. Support multiple AWS accounts.

199. Your security department has approached you wanting to have a centralized view of all identified network threats in your AWS environment. What would be the best product to give them that visibility?

A. Amazon Inspector

B. AWS Trusted Advisor

C. Amazon GuardDuty

D. Amazon QuickSight

200. Your security department has approached you about monitoring suspicious user activity in AWS. What would be the best product to give them that visibility?

A. Amazon GuardDuty

B. AWS IAM

C. AWS Directory Service

D. AWS Organizations

201. Which product provides the fastest performance when you need to run a large report that includes complex queries?

A. Amazon EMR

B. Amazon RedShift

C. Amazon Athena

D. Amazon RDS

202. Which AWS product is best suited to replace an on-premises data lake using Hadoop?

A. Amazon EMR

B. Amazon RedShift

C. Amazon Athena

D. Amazon RDS

203. You need to be able to run ad hoc queries against data in Amazon S3. Which product is best suited for this task?

A. Amazon EMR

B. Amazon RedShift

C. Amazon Athena

D. Amazon RDS

204. You are using Amazon Kinesis Firehouse to collect a large amount of data in real time. How can you analyze the data if it is stored in Amazon S3 in a cost-effective manner?

A. Amazon RDS

B. Amazon CloudWatch

C. AWS Lambda

D. Amazon Athena

205. What is a benefit provided by Amazon Macie?

A. Performing security assessments in AWS

B. Visibility into the locations where you store data

C. Running ad hoc queries against Amazon S3

D. Management of storage encryption keys

206. What is a benefit provided by Amazon Macie?

A. Monitor API usage for storage access.

B. Manage storage versioning in S3.

C. Integration with Amazon CloudWatch Events

D. Manage the storage lifecycle in S3.