

AWS Security Specialization Certification: Little Guide

Version: 1.0.0

HadoopExam Learning Resources

Contents

Topic-1: KMS: Key Management Service
Topic-2: AWS VPC
Topic-3: S3: AWS Storage
Topic-4: AWS Permissions using Policy
Topic-5: AWS Monitoring
Topic-6: AWS CloudHSM
Topic-7: AWS CloudWatch
Topic-8: AWS WAF
Topic-9: AWS Config
Topic-10: AWS Lambda
Topic-11: AWS Secret Manager
Topic-12: AWS EC2
Topic-13: AWS Security in General
Topic-14: AWS Inspector
Topic-15: AWS Trusted Advisor
Topic-16: AWS CloudTrail
Topic-17: AWS Certificate Manager
Topic-18: AWS System Manager Patch
Topic-19: AWS Shields
Topic-20: AWS EBS
Topic-21: AWS Organizations
Topic-22: AWS & DDoS Attack
Topic-23: AWS CloudFront
Topic-24: AWS API Gateway

About Book

This book is for preparing AWS Certified Specialty (SCS-C01) examination. In this book we cover important points regarding the certification exam, it is not a complete study guide and does not provide any hands on practical material. We tried to keep this book as short as possible and tried to cover all aspect of the examination. So that in lesser time you can revise this book 3-4 times before your exam. This book must be used in conjunction to [AWS Certification Simulator](#) (Contains questions for certification exam). We will be keep updating this book time to time, hence if you have bought this book from <http://HadoopExam.com> then future updates on this book will are free. This book covers various topics related to certification exam and important concepts on that particular topic which you must understand in detail. Because in AWS certification exam, questions are concepts and design based they never asks direct questions and have big pool of questions. So if you know the concepts and how to properly use AWS services in secure manner. You can easily answer questions during your real exam.

About SCS-C01 certification exam

AWS Certified Security Specialty (SCS-C01) exam is for the developer, architect to prove that they can design and AWS services in secure manner. And even if you are a security professional then by doing this certification you can add one more star in your profile and career growth. If you see the syllabus for this exam it is mentioned very abstract, and difficult to find what to study they have not mentioned the service wise topic. That's the reason HadoopExam come up with this book and tries to cover the specific topic and reduce your overall preparation time for the exam. Yes, it is true that AWS documentations are very good and in detail, but by reading those documentations will take very long time and even it is difficult to find what to skip and what to focus. Current syllabus for the exam

Domain 1: Incident Response (12%, 7-9 Questions)

- Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys.
- Verify that the Incident Response plan includes relevant AWS services.
- Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.

Domain 2: Logging and Monitoring (20%, 13-14 Questions)

- Design and implement security monitoring and alerting.
- Troubleshoot security monitoring and alerting.
- Design and implement a logging solution.
- Troubleshoot logging solutions.

Domain 3: Infrastructure Security (26%, 16-18 questions)

- Design edge security on AWS.
- Design and implement a secure network infrastructure.
- Troubleshoot a secure network infrastructure.
- Design and implement host-based security.

Domain 4: Identity and Access Management (20%, 13-14 Questions)

- Design and implement a scalable authorization and authentication system to access AWS resources.
- Troubleshoot an authorization and authentication system to access AWS resources.

Domain 5: Data Protection (22%, 14-15 Questions)

- Design and implement key management and use.
- Troubleshoot key management.
- Design and implement a data encryption solution for data at rest and data in transit.

About AWS® Certified Security Specialty (SCS-C01) Certification Simulator: All Questions with detailed explanation: Without security software world cannot survived, security specialization in a particular field give you an edge in your career and one of the most reputed career choice. This particular certification is useful if you are a security professional and already working in security world or trying to enter in this world. If you are a security professional entire organization has to follow the standard specified by you. As you know in the Cloud Computing world AWS is pioneer and no one close to this platform. It is easy to create and design solution in AWS, but it required a very good knowledge for creating a well-designed security platform. And one of the best way to prove you are well versed with the AWS secure infrastructure design which is also compliant as per HIPAA, PCI, other financial regulatory specification. After completing this certification you can prove that you are good at data protection, data encryption, and secure communication over internet, various AWS security services, creating secure production environment, taking good decision for cost, security, complex secure deployment, and secure operations and how to mitigate all the risks associated with design. You can check what all is covered for the exam. Now the problem is that exam syllabus is so abstract what to read and what all services needs to focused is not clear. But HadoopExam brings you question with specific topic as well as how multiple services are combined together to create a secure solution on AWS. Each question comes with the detailed explanation. So now start preparing with premium material for HadoopExam Learning Resources.

Topic-1: KMS: Key Management Service

About KMS: Key Management Service, as name suggests it for managing keys, provided by AWS. It is the responsibility of AWS for availability, physical security, and control of the keys access and maintenance of the KMS infrastructure. Also using CloudTrail logging you can find that by whom and when keys from KMS are used. Basically this service is helpful in encrypting the data like data stored in S3 bucket, if you want encrypt than you can use this service, similarly creating encrypted EBS volume (Data stored on EBS) will be encrypted.

Customer Master Key: This is the key which will be stored in KMS (Also known as CMK) and will be identified using ARN or KeyId. When keys are rotated it means underline contents of CMK will be changed or updated, because CMK itself is container.

Data Key: CMK is a container for Data Key, and Data Key (in plain text format) is used to encrypt data (e.g. stored in S3 bucket or encrypting EBS volume). You will be storing data key in encrypted format with your data and whenever you want decrypt the data, you will send this encrypted data key to the KMS (CMK) and then KMS will return plain text of the Data Key. Now using this plain text Data Key you can encrypt or decrypt the data. CMK never stores data keys in either form. To get data key you have to use TLS/SSL channel.

Exam Point: CMK is managed by the KMS, which encrypts the Data Key. Data Key is never stored CMK. CMK never ever leave the KMS, you can only get the Data Key from the KMS.

Ciphertext: It is an encrypted data.

Envelop Encryption: Important points to remember in this case is that the key stored in KMS are not actually used for encryption of your data rather you will be using another key that is known as data key to encrypt the data. This data key is encrypted and decrypted using Master keys (KEK: then this master key will be known as Key Master Key) are stored in KMS. KMS never store data key and data, it only store master keys (CMK). However, you can provide your own master key as well, which is known as Custom Customer Master Key (C-CMK) and another type of master key is generated by AWS itself and master key generated by AWS will never leave KMS infrastructure. In simple term

- Ciphertext/encrypted data = Encrypt(Data Key, data)
- Encryption Key/encrypted data key = Encrypt(master key, data key)
- Create envelop = (Encryption key, Ciphertext) and keep them together.

Now you need master key to get data key. This master key can be retrieved from KMS. If you need client side envelop encryption then you have to use AWS Encryption SDK.

Encrypted data across region: If you have used Envelop encryption then you can transfer encrypted data to another region as it is. And whenever you want to decrypt this data in another region, just get the plain text copy of your data and use it in another region.

Exam Point: You can use encrypted data using KMS in another region as well. By transferring your plain text data key to another region.

For encryption you will have following types of keys

A. Master Keys

- a. Provided by user/customer known as Customer managed CMKs
 - i. A customer managed CMK is created at your request.
 - ii. These keys are rotated automatically.
 - iii. You can delete the customer managed CMK.
 - iv. You can either ask AWS to create key material or you can import your own key material.
 - v. User Provided Key material
 1. If you provide key material then you can set its expiration, you can delete them or even re-use them in future.
 2. You can also store it outside KMS.
- b. **Generated by AWS:** This key will never leave KMS and known as AWS managed CMKs.
 - i. AWS managed CMK will be created when you choose to enable server-side encryption on an AWS resource under the AWS managed CMK for that service first time also known as SSE-KMS.
 - ii. AWS managed CMK are specific to an account and a region.
 - iii. AWS managed CMK can be used only for resource for which it is created like S3. You cannot use same AWS managed CMK for both S3 and Redshift cluster. You must have separate CMKs for both the resource.
 - iv. If you need more granular control then rather use Customer Managed CMKs.
 - v. AWS managed CMK is automatically rotated in every 3 years.

- vi. You cannot delete AWS managed CMK
- vii. Key access policies are also managed by AWS

B. Data Keys

- a. **Plain Text Data Key:** This is the key you will use to encrypt and decrypt your data. This data keys are generated in HSM(Hardware Security Manager). You can get this data key from KMS in plain text as well as encrypted form.
- b. **Encrypted Data Key:** This is an encrypted version of plain text data key, which always remain with the data. With the encrypted data key you cannot decrypt the data. You have to first decrypt data key using master key, which will give your original plain text data key and this data key will be used to encrypt and decrypt the data. Once you are done with encryption and decryption immediately delete this data key.

Points to remember:

1. AWS uses the Hardware Security Module to protect master keys.
2. Master keys (CMK: Custom ~~not customer~~ Master key) never leave the KMS, if generated by AWS integrated service.
3. You will never be using master keys to encrypt your data, why?(See below).
4. You will not send data to KMS for encryption.
5. Data will be encrypted using data key and data key itself will be encrypted using master key. Hence, you will be sending Data key to KMS, where it will be decrypted or encrypted as per the need.
6. Even using IAM users and roles you can manage that who can access your master keys and who cannot access the master keys.
7. AWS maintains the entire logging/audit of the use of master keys in KMS. This logging will be available using CloudTrail, and help you for compliance and regulatory needs. CloudTrail is a service which will store log files in a specified S3 bucket.
8. **Envelop encryption :** Encrypting data using data key and encrypting data key using master key is known as a envelop encryption.
9. Managing data keys are not the responsibility of the AWS KMS, it rather yours. Even AWS does not do cryptographic operations with the data keys.
10. There are two types of master keys(Custom master keys)
 - a. Customer managed master key(CMK) :
 - i. This key is created, managed and used by you.
 - ii. You can enable and disable the CMK.
 - iii. You can create IAM policies to control the access.
 - b. AWS managed master keys (CMK)
 - i. This are managed by AWS, and will be used by AWS services like S3, Redshift on your behalf.
 - ii. This CMK is unique to your AWS account and region.
 - iii. It can be used by only service, which created it like S3 created a CMK then only S3 service can use it. Hence, KMS and AWS service are well integrated.
11. **Cipher text:** Your plain text data, when encrypted using plain text data key and with an encryption algorithm. And generate an encrypted data, this encrypted data is known as a Ciphertext.

12. **Permissions:** There is a policy attached to CMK, to define the permission to use and manage CMK.
13. **Key Policies:** It is a document in which you will add policy, which defines who can add, remove and modify permissions for customer managed CMK (I am repeating, its customer managed only). You cannot edit the key policy for an AWS managed CMK.
14. **Grants:** It is an alternative to Key Policy to give long-term access to AWS Principals to use your customer managed CMKs.
 - a. You can use grants in Key policy document when you want to give temporary permission or delegate permission for other principals to use your CMK on your behalf in the absence of direct API call from you.
15. In cryptography two things are involved Encryption Algorithm (Its public) and Secret keys (It must not be public and kept safe). AWS KMS is the solution for keeping this secret master keys safe and they never leave KMS in case of AWS service.
16. While creating CMKs from console, you can assign which external users (other AWS users) can access master keys, but the administrator of external users also allows access to an external account by creating IAM polices. **So just by providing access to master keys by you is not enough.**
17. **Remember:** CMKs are specific to an account and a region. Hence, will not be available across regions even for same account (In case of AWS Managed CMK).
18. **Editing master keys:** You can edit the some of the properties of Customer Managed CMKs, but not the one which is managed by AWS. For example you can change the description, add and remove administrator and users, manage tags, enable and disable key rotations.
19. **Deleting master key:** If you don't want that your administrator can delete the master key then you have to un-check the box in console which says "Allow key administrators to delete this keys"
20. **You cannot tag the AWS managed master keys.**
21. Changing the status of master keys:
 - a. You can only enable and disable customer managed master keys.
 - b. You cannot changes the status (enable and disable) AWS managed keys. They are permanently enabled and cannot be disabled.
22. **When keys are in disabled status, they cannot be used for encryption.**
23. **When keys are in disabled state they cannot be rotated.**
24. To control the access of KMS you can use IAM, who can access CMKs.
25. You must need permissions to create KMS CMK, manage a CMK, and to use CMK for cryptographic operations such as encryption and decryption.
26. In KMS **primary resource type is Customer Master Key** and another resource type in KMS which can be used with CMK is alias, which is a friendly name to CMK.
 - a. CMK Key
 - b. CMK Alias
27. The primary way to manage access to your KMS CMKs is using policies. Policies are documents which describe who can access what. So you can use alias name to work with the KMS.
28. **Policies:** It is a document that describe who has access to what.
 - a. **Identity based policy :** It is attached to IAM identity (Role, User and Group)
 - b. **Resource based policy:** Attached to an AWS resource like KMS.

29. **Remember:** CMKs aliases cannot be used within policy document, because it can change outside the policy. Hence, Key ID should be used in Key policies.
30. Policies are attached to IAM Identity like (Users, Groups or Roles) then it is called Identity-based-policies.
31. If policies are attached to AWS resources then those are called resource-based-policies.
32. In AWS KMS, you must attach resource-based policies to your customer master keys (CMKs) and these are called Key policies. And remember all CMKs have key policy attached.
33. **Controlling Access to AWS KMS CMKs:** You will be using following ways to control access to a CMK.
- Using Key Policy:** You can use single Key Policy document to define the access control.
 - IAM Policy + Key Policy:** In this way you can manage all of the permissions for your IAM identities.
 - Grant + Key Policy:** You can use grant and Key policy to allow access to CMK. In Key policy you control the access to the CMK and also allow users to delegate their access to others.
34. **Remember:** To allow access to KMS CMK, you must use Key Policy (Remember: That is a mandate). You can use any of the above combination to control the access to CMK. IAM policy alone are not enough to control the access for CMKs. For most of the other services IAM policies are enough but this is not the case with KMS.
35. A key policy will be applied to only to the CMK it is attached to.
36. **Key Policy and Principal:** Principal are the main identity which gets permissions, which are specified in Key Policy document for example root user, IAM user, IAM roles and AWS services. But remember IAM groups are not valid principal in a key policy. As groups are not allowed you can use multiple users in key policy.
37. Default Key Policy gives the root AWS user who owns the CMK full access to CMK.
38. **CMK Administrator:** You can choose IAM users and roles in the account and make them key administrator. Key administrator have permissions to manage the CMK, but do not have permissions to use the CMK to encrypt and decrypt the data. But they can modify the key policy, so that they can give permissions to themselves to use it for encryption and decryption.
39. If you are a key user than you can delegate the permissions to other users as well, so they can use it. For example
- Implicit permission to EC2:** If you want to attach encrypted EBS volume to EC2 then use CMK with EBS (Elastic Block Storage).
 - Launching encrypted Redshift cluster:** If you are creating a Redshift encrypted cluster then it uses the keys owned by you implicitly to launch the cluster and also snapshots created will be encrypted.
40. **Default Key Policy:**
- If you want to delegate the permissions to other user to use CMK with other AWS integrated services, then it cannot be selected service it can be either all services or none.
 - If you want to give permission for selected AWS integrated service than you have to use custom key policy.
41. **Key Users:** You can add IAM users, IAM Roles and external AWS accounts to the list of key users.
42. **IAM Policy vs Key Policy Principal:**

- a. **IAM Policy:** You don't specify principal but rather specify IAM User, Groups and Role.
 - b. **Key Policy:** In a Key policy, you must specify the Principal/Identity on which permission needs to be applied. You can specify AWS root account, IAM Users, IAM Roles and Some AWS services as principal. **However, note that IAM groups are not valid Principal in Key Policy.**
43. **Data Key:** This is the key which you will be using for encrypting the data (It is a plain text key) and not the CMKs. CMKs can encrypt only 4 KB data at a time and CMK can never leave KMS. Hence, you will send Data Key to KMS which will encrypt your data key. So you will be following below steps for encryption.
- a. Using Data Key (Plain Text) encrypt your data.
 - b. Using CMKs you will encrypt your plain text data key.
 - c. Delete the plain text data key.
 - d. Save encrypted data key with the encrypted data.
 - e. Using encrypted data key data cannot be decrypted. First data key needs to be decrypted using CMKs. Once data key is decrypted which again gives you plain text key, using that decrypt your data.
 - f. A CMK can be used to directly encrypt data blocks of upto 4KB or it can be used to secure data keys.
44. **KMS users:** There are following types of key users
- a. **Key Administrator:** This users/roles can administer the key. If you allow they can even delete the key.
 - b. **Key users:** This users can use this keys to encrypt and decrypt the data key from within the application.
45. To change the permission you have to modify key policy documents.
46. **Adding External AWS Account to Key Policy:** If you add external AWS accounts to a key policy, you must also use **IAM policies in the external accounts to give permission to IAM users, groups or roles in those accounts.** For example **HadoopExam_CMK_Owner** who owns the CMK and **HadoopExam_CMK_User** wants access to CMK.
- a. **Step-1:** Modify **key policy** for the CMK in account **HadoopExam_CMK_Owner** so that external account owner e.g. Root user can be added. This external account can be a Key Administrator as well.
 - b. **Step 2:** Add/Modify an IAM policy attached to users in account (root/owner account) **HadoopExam_CMK_User**. IAM Policies do not contain the Principal element, which differs from KMS Key Policies. In IAM Policies principal is implicit to which this policy is attached.
 - c. Hence, we have to modify both Key Policy(attached to CMK) as well as IAM policy attached to the user.
47. If you are not able to modify key policy properly using AWS console, it means these keys policy was not created using AWS console or it had been modified in a way that the console default view does not support it.
48. **Permission to multiple users using IAM Groups:** You need to follow below approach
- a. Add each IAM user to the key policy.
 - b. **In Key Policy:** Enables IAM Policies to allow access to the CMK.
 - c. Create an **IAM Policy** that allow access to CMK.

- d. Attach this Policy to an IAM group which has users from step a.
 - e. Hence, if users change then you need to update group and key policy.
49. **Remember:** for KMS IAM policy alone is not enough. You need IAM Policy + Key Policy or Only Key Policy is enough for permissions.
50. **In IAM Policy:** A policy that explicitly denies the permissions overrides all other policies, even those that explicitly allow the same permissions.
51. **Condition statement in policy document:** If you want that permissions can be enabled based on condition like statement should be effective after a particular date or specific value appears in a specific API. Then use condition statement in policy document.
52. **Caution with IP address based conditions:** Suppose you create an IAM policy and specify a range of IP address from where it can use AWS services like EBS, EC2 and KMS. Now this same IAM user attempts to attach an encrypted volume to an EC2 instance and action fails even user has permission on all three required services.
- Reason:** Request reaching to KMS to decrypt the volumes encrypted data key comes from the IP address of EC2 instance which does not allow IP addresses other than specified in the Policy Document.
53. **Remember:** If you are using aws:sourceIP based condition to restrict IP addresses, even then if request comes from AWS VPC Endpoint condition key will not be effective. You have to use aws:sourceVPC condition keys in this case.
54. **EncryptionContext:**
- a. It is an additional layer of authentication for your KMS API calls.
 - b. It is just a key-value in plain text format. Hence, whenever you call API for encryption and decryption you must send this key-value with the API call.
 - c. It is plain text key-value, so you must not use sensitive information in this.
 - d. If you use encryption context during encryption then it is also required during decryption context.
 - e. Encryption context (Key-value) is also logged in CloudTrail logging.
 - f. An encryption context is a set of non-secret key-value pairs that you can include in a request for any AWS KMS cryptographic operations like encrypt, decrypt, re-encrypt and generate data key. Hence, whenever you apply encryption with encryption context then while doing decryption also you have to provide encryption context. Otherwise decryption request will fail. Encryption Context keys are used as part of Condition in policy document example below.
- ```
"Condition": {
 "StringEquals": {
 "kms:EncryptionContextKeys": "HadoopExamAPP"
 }
}
```
- In above case, it expects that request come with "HadoopExamAPP" as an EncryptionContextKey and StringEquals in condition also want that it is case sensitive.
- g. In case of EBS sends VolumeID as the encryption context while cryptographic operations for a volume, and while taking snapshot it uses snapshot ID for the context. If AWS does not use the encryption context in this situation then EC2 instance will be able to decrypt any EBS volume under that specific CMK.
55. **Important points about Key Policy:**
- a. Policy attached to IAM Identities (Users, Groups and Roles) are called Identity based policies or IAM Policies.

- b. **Resource based policies:** Policy attached to resources are known as resource based policy. KMS is an AWS resource, hence you will attach resource based policy to it and this is also known as key policy.
  - c. All CMK will have a key policy and it is must you use it to control the access.
  - d. IAM policy alone is not enough for KMS CMKs permissions.
  - e. IAM policies are based on default-denied unless you explicitly grant permission to a principal to perform an action.
  - f. **Key policy:** They are the primary for controlling the CMKs access.
  - g. Each CMK will have key policy attached to it either default one or modified by you, which specify who can use or manage it.
  - h. User or application who want to use encrypted resources than he must have access to both keys and that particular resource like S3, Redshift cluster, EBS etc.
  - i. In the policy document you can control that any specific service can only use CMKs like only by S3 for that you have to use policy document and in that document you have to specify that kms:ViaService condition.
  - j. If you want that other AWS services or application can use your keys on your behalf then you have to use Grants actions in the policy documents. And with the condition you will make sure that which service e.g. EC2 can use this service.
  - k. Hence, in a key policy document you will have
    - i. **Resource** :Which AWS resource can use KMS e.g. EC2 instance
    - ii. **Action:** What action a Principal can take for the KMS e.g. RevokeGrant
    - iii. **Effect:** Whether it's allow or deny.
    - iv. **Principal:** It can be a role or user
    - v. **Condition:** To use KMS condition provided here must be satisfied.
  - l. You can specify that Key administrator can only manage the keys but cannot use the keys for encryption and decryption of the data.
56. You can even use MFA for additional layer of security. You have to use condition in key policy document to enable MFA, it is usually give 5 minutes time for MFA.
57. **Detective control and KMS:** It helps in configuring KMS to log all the required information for auditing.
- a. **Enable CloudTrail:** To audit the usage of your keys in AWS KMS, you should enable CloudTrail logging in your AWS account.
  - b. **Logging files:** All the logging files from CloudTrail will be delivered in S3 bucket.
  - c. **Cloudwatch and KMS:** KMS can also emits the Cloudwatch events when CMK rotated, deleted or key material is imported.
58. All request to KMS must be over the TLS and terminate at KMS host.
59. You can never export plain text format of CMKs from KMS.
60. **Key material:** AWS KMS provides an option to import key material.
61. **KMS support only symmetric encryption and decryption.**

#### VPC and KMS:

- A. **If you want more security than you can connect to KMS via a private endpoint in VPC and avoid connecting to KMS over the internet.**

- B. AWS KMS support VPC interface endpoints that are powered by AWS Private Link.
- C. Each VPC Endpoint is represented by one or more ENI (Elastic Network Interface) with private IP address in your VPC subnets.
- D. The VPC interface endpoint connects your VPC directly to AWS KMS without having an internet gateway, NAT devices, VPN connection or AWS Direct connect connection.
- E. Instances in your VPC do not need public IP address to communicate with AWS KMS.
- F. While doing KMS API or CLI commands, you have to provide endpoint-url, which specifies a VPC endpoint.
- G. **VPC Endpoint and DNS hostname:**
  - a. If you use the default domain name servers (Amazon Provided DNS) and enable private DNS hostnames for your VPC endpoints, then you can avoid providing VPC endpoint URL in your API or CLI command.
  - b. In this case AWS populates your VPC name server with private zone data, so that public KMS endpoint which is <https://kms.<region>.amazonaws.com> resolves to your private VPC endpoint.
  - c. To enable this feature while using your own name servers, forward request for the KMS domain to the VPC name server.
  - d. You can also use AWS CloudTrail logs to audit use of KMS keys through the VPC endpoint. By doing this you can use conditions in IAM and Key Policy to deny access to any request that does not come from a specified VPC or VPC endpoint.
  - e. **Key policy and VPC Endpoints:**
    - i. As mentioned previously you can use condition keys in KMS Key Policy to restrict access to the AWS KMS CMKs to request from the VPC and VPC endpoints. Using sourceVpc or sourceVpce
    - ii. However, using this conditions that allows and denies access to AWS KMS CMKs, you might inadvertently deny access to KMS on your behalf.
    - iii. Take care to avoid a situation like the IP address condition keys example. If you restrict requests for a CMK to a VPC or VPC endpoint, calls to AWS KMS from an integrated service, such as Amazon S3 or Amazon EBS, might fail. This can happen even if the source request ultimately originates in the VPC or from the VPC endpoint.

#### Tags and Cost:

- You can use AWS resource tags to generate cost allocation report which can be aggregated based on tags.
- Hence, whenever you need cost report for individual department, under single AWS root account. It is the best strategy to use.

#### S3 Bucket:

1. You will never be encrypting entire S3 bucket. Rather contents in the bucket will be encrypted.
2. You can use S3 bucket to store secrets and apply bucket policy so that only authorized individual/application/roles can access the buckets. Enabled CloudTrail logging on the bucket.
3. You can create policy in S3, which does not allow un-encrypted data.

#### AMI, EBS and Data encryption:

1. You can create AMI which can use encrypted EBS boot volume and this AMI can be used to launch EC2 instances.
2. So data which is stored is also encrypted as well as data transfer between EBS and EC2 is also encrypted.
3. This feature will use KMS, so every use of KMS will be audited.
4. **Server Side EBS Encryption:**
  - a. EBS will get encrypted volume key from CMK and store it in EBS volume metadata.
  - b. While mounting EBS volume, encrypted volume key will be fetched from metadata.
  - c. Now call KMS over TLS/SSL to decrypt encrypted volume key. AWS KMS finds the CMK for encrypted volume key (data key) and asks HSM to decrypt the volume key.
  - d. KMS will return this decrypted volume key to EC2 instance over SSL/TLS.
  - e. This volume key (plain text) will be used to encrypt and decrypt the data which in/out to attached EBS volume. Encrypted volume key remains with the EBS metadata.
5. **Client side data encryption:** You have to use AWS Encryption SDK for that and it will use Envelope Encryption for that.
  - a. Request for new data key under a CMK from KMS. You will get encrypted+ plain text data key.
  - b. In SDK you have to use plain text data key to encrypt the data. Once encryption is done delete plain text key.
  - c. Store both encrypted data key and encrypted data together called envelop.
  - d. For decryption SDK will get encrypted data key from envelop and ask KMS to decrypt this data key.
  - e. SDK will get plain text data key from KMS.
  - f. This data key can be used to decrypt the data. Once done delete the plain text key.

#### **Lambda and EBS encrypted volume:**

1. You can monitor the creation of EBS volume, as soon as EBS volume is created an event will be logged in CloudTrail log.
2. Then based on this event a Lambda function needs to be triggered by CloudTrail event to check whether EBS volume is encrypted or not and also what KMS was used for encryption.
3. Based on this Lambda can take various actions like if volume is not encrypted then delete EC2 instance and quarantine the instance by blocking all inbound connection using Security Group.
4. Send an alert to SNS etc.

#### **RDS and Encryption:**

1. RDS builds on EBS encryption to provide full disk encryption for database volumes.
2. When you create an encrypted database instance with AWS RDS, RDS will create an encrypted EBS volume on your behalf to store the database.
3. Data stored in the form of volume, snapshots, backups, and read replicas all are encrypted under the KMS CMK.
4. Based on this you can set up Lambda function call as well, to monitor the creation of new RDS instance.

#### **KMS and Lambda:**



- If you detect any issue with the KMS, then configure the Lambda accordingly to take the action automatically.

#### **CMK deletion:**

- Once CMK is deleted from KMS than it is gone for forever.
- **So rather than deleting the keys, you need to first consider them for disabling. Once you are sure that it is nowhere used than consider to delete it.**
- **Pending deletion:** AWS gives you chance up to 30 (configurable) days once the key is deleted to recover it. But when key is in Pending deletion state it cannot be used for encryption and decryption, you have to cancel the deletion first to use it. After this many configured days key will be deleted forever and cannot be recovered.
- You should use MFA for deletion CMKs. Because once key is deleted it can never be recovered and encrypted data cannot be encrypted again.

#### **KMS Lambda variables:**

1. By default AWS Lambda variables are encrypted using KMS.
2. You have an option to use the default KMS key for Lambda or specify a specific CMK of your choice.

#### **Secure String:**

1. A secure string is a sensitive data that needs to be stored and referenced in a secure manner e.g. clear text password.
2. If you don't want this secure string to be presented as clear text in commands, functions, agent logs or CloudTrail logs. Then in this case also KMS can be used, you can use AWS provided or your own provided KMS.

#### **Access Keys:**

1. AWS access keys can be used to access AWS resources programmatically, through one of the AWS SDKs or command line tools.
2. SDKs and command line tools can use access keys to cryptographically sign API requests.
3. If you don't use SDK or command line tools, then you must sign API requests yourself.

#### **IAM Roles:**

1. Similar to IAM user, you can assign permissions to IAM roles as well.
2. IAM roles are similar to IAM user, but they are not associated with a specific person.
3. Using IAM Role you obtain temporary access keys to access AWS resources/service programmatically.
4. IAM Roles are useful in following situation.
  - a. **Federated User Access**
    - i. If your organization is already using solution like LDAP or Microsoft active Directory, or any other identity provider for users access management. Then this users are known as federated users.
    - ii. This federated users can use Identity Provider.

**b. Cross Account access**

- i. You can use an IAM Role in your AWS account to allow another AWS account permissions to access your account resources.
- ii. If you add root account in a key policy then he can delegate the permissions to a CMK within KMS to other user or role within its own account using IAM policies.

**c. AWS Service access**

- i. If you want one service in your account can access another service. Then you can use IAM Role for that. Suppose you have to load data from S3 to Redshift cluster. Rather than using your account credentials, you will be using an IAM Role which allows Redshift to access S3 bucket on your behalf. So that it can load data from S3 bucket to Redshift cluster.

**d. Applications running on EC2 instances**

- i. If you have created an application which is running on EC2 instance. Application need to access AWS resources programmatically. It is not a good idea to store your access keys on EC2 instance.
- ii. You should assign an IAM Role to an EC2 instance.
- iii. To assign a Role to an EC2 instance, you will be creating an instance profile and then attach this profile to an EC2 instance while launching it.
- iv. An instance profile contain the role and enables application running on EC2 instance to get temporary access keys.

**5. Permissions Policies:**

- a. Every AWS resource belong to an AWS account, and permission to create or access these resources are defined in permission policy of that account.
- b. An account administrator as well as some AWS services like KMS can add permission policies to IAM Identity e.g. users, groups and roles.

**KMS and Master Key Rotation:**

1. To create a new cryptographic material for KMS CMKs, you can create new CMKs and then change your applications or aliases to use new CMKs or it can be enabled for automatic key rotation for an existing CMK.
2. **Customer Managed CMK:** If automatic key rotation is enabled for customer managed CMK. Then new cryptographic material will be generated every year by AWS KMS.
  - a. In this case KMS will store older cryptographic material, hence older data can be decrypted. Once you lose CMK you can never decrypt the data.
3. CMK is a logical container for cryptographic material. Hence, only cryptographic material is rotated.
4. What happen after key rotation:
  - a. Properties of CMK e.g. ID, ARN, region, policy and permission remain same.
  - b. We don't have to change application or aliases that refer to the CMK ID or ARN.
  - c. Rotation will happen every year, no need to remember the schedule.
5. **Important:**
  - a. Automatic rotation has no effect on the data that the CMK protects.
  - b. It does not rotate data keys, and not even touches already encrypted data.
  - c. If you have compromised data key than data encrypted using that key are on risk.



6. You can even use manual rotation of the keys, if you want rotation as per your schedule and you can use your own key material in this case.
7. Rotating customer managed CMKs can incur extra monthly charges.
8. **Backing Keys and KMS:**
  - a. KMS always retain backing keys.
  - b. Backing key can only be deleted when CMK is deleted.
  - c. While encrypting KMS always uses the current backing keys, and while decrypting it will use the key which was used for encryption.
9. If Key Material is imported than automatic key rotation is not available. (If you see origin field as external).
10. AWS managed KMS key rotation will happen every three years which is equal to 1095 days.
11. Replacing one CMK with another CMK is known as manual key rotation. In case of imported key material this is a good choice for key rotation. You should keep both old and new CMK, otherwise you will not be able to decrypt data which was decrypted with the previous keys.
12. As you are replacing old CMK with the new CMK manually than you have to change CMK ID or ARN in your application as well. Better solution for this is to use aliases.

**Premium Trainings Courses :** HadoopExam focuses on in depth learning with the hands-on session setting up the environment than executing solution and doing hands on that. Below are the available trainings and we are keep adding new trainings. These trainings is being used and subscribed by Developer, Tester, Administrator, Enterprise(to train their team) and Trainer globally. These trainings are well organized and step by step solutions to learning, and in lesser time as per your convenience you can complete these and even re-visit as required.

All Premium Training Access Annual Subscription (You will get early access to under development training and early edition books) : Used By More than 20000 subscribers

|                                                                                                                                                       |                                                                                                                                                                                                                      |                                                                                                                                                                      |                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Spark Professional Training : HandsOn</b><br><a href="#">CLICK HERE</a><br><a href="http://HadoopExam.com">HadoopExam.com</a><br><b>32 Modules</b> | <b>Spark 2.x SQL Training: HandsOn</b><br>Good for Data Analytics, Developer Data Science<br><a href="#">CLICK HERE</a><br><a href="http://HadoopExam.com">HadoopExam.com</a><br>19-Modules<br>37-Hands On Exercises | <b>NiFi : Hortoneworks DataFlow (HDF) Hands On Training</b><br><a href="#">CLICK HERE</a><br><a href="http://HadoopExam.com">HadoopExam.com</a><br><b>16 Modules</b> | <br><a href="#">Click Here</a><br><b>Hadoop Training With HandsOn</b> |
| <br><b>Admin</b><br><a href="#">Click Here</a>                      | <br><a href="#">Click Here</a>                                                                                                     | <br><b>BASE Training</b><br><a href="#">Click Here</a>                             |                                                                                                                                                          |
| <b>Cloudera Hadoop Admin Training Course-1</b>                                                                                                        | <b>HBase Professional Training</b>                                                                                                                                                                                   | <b>35 Hands On Sessions<br/>20 Module</b>                                                                                                                            |                                                                                                                                                          |

|                                                                                                                                                                                              |                                                                                                                                                                                                                                |                                                                                                                                                                                                              |                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p><b>CLICK HERE</b></p> <p>HadoopExam.com</p> <p>22 Modules</p>                                           |  <p><b>CLICK HERE</b></p> <p>HadoopExam.com</p>              |  <p><b>Click Here</b></p> <p>Training :<br/>Core Java<br/>120-808</p> <p>HadoopExam.com</p>                                 |  <p><b>Click Here</b></p> <p>Training :<br/>Scala Professional :<br/>Hands On</p> <p>HadoopExam.com</p> |
|  <p><b>Click Here</b></p> <p>Training :<br/>Professional :<br/>Training : HandsOn</p> <p>HadoopExam.com</p> | <p><b>Book</b></p> <p>Spark SQL 2.x<br/>Fundamentals &amp;<br/>Cookbook</p> <p><b>READ NOW</b></p> <p>HadoopExam.com</p> <p>Pages : 158</p>  | <p><b>Book</b></p> <p>AWS Solution Architect<br/>Associate : Little Guid</p> <p><b>READ NOW</b></p> <p>HadoopExam.com</p>  | <p><b>Book</b></p> <p>NiFi CookBook :<br/>HandsOn Exercises</p> <p><b>READ NOW</b></p> <p>HadoopExam.com</p> <p>Pages : 130</p> <p><b>NiFi</b></p>                                         |

**Apache Spark Training & Certifications:** Apache Spark is new and fastest data processing engine for Big Data world, after Hadoop it's becoming more popular in Industry (recently demand increased a lot). Now using power of Hadoop and Spark. Hence, data processing speed has dramatically increased. So if you wish to work in/with Big Data then Learning Spark is a must even for becoming data scientist., HadoopExam Learning Resources launched low cost material for in depth learning of Spark in the form of Spark Professional Training with Hands on practice sessions and helping you to get certified with most popular Apache Spark Certification conducted by Oreilly and Databricks only. So without delaying start preparing or prove your skills of Apache Spark, subscribe to our trainings and certification material with special discount of unbeatable price. You can request free updates as well, whenever it is done.

New  
**Spark 2.x**  
360 Q&A + 15 Videos  
[Click Here](#)

New  
**PySpark 2.x**  
120 Q&A  
[Click Here](#)

**APACHE Spark**  
300 Q&A  
[Click Here](#)

**HORTONWORKS**  
65 Solved Scenarios  
[Click Here](#)

**Databricks Certified Developer Spark 2.x for Scala**

**Databricks Certified Developer Spark 2.x for Python**

**Oreilly™ Spark Developer Certification**

**HDPCD-Spark Developer Exam**

**hadoop**  
95 Q & A  
[Click Here](#)

**MAPR**  
220 + Q & A  
[Click Here](#)

**Cloudera Hadoop & Spark Developer CCA175**

**MCSD : MapR Certified Spark(Scala) Developer**

1. [Databricks Spark 2.x Spark Developer Certification Scala](#)
2. [Databricks Spark 2.x \(PySpark\) Developer Certification Python](#)
3. [Apache Spark Professional Training with Hands On Lab Sessions](#)
4. [Oreilly Databricks Apache Spark Developer Certification Simulator \(Retired\)](#)
5. [Hortonworks Spark Developer Certification](#)
6. [Cloudera CCA175 Hadoop and Spark Developer Certification](#)
7. [MCSD : MapR Spark \(Scala\) Certified Developer](#)

---

**Cloudera® Certifications Preparation Kits and Trainings:** Cloudera is a pioneer for Hadoop Big Data framework and they have grown a lot since last a decade. Cloudera® solutions is being used a lot in industry. They had also converted all their certification exam from multiple choice to Hands-on exam. HadoopExam was the first one, who launched Cloudera certification material 5 years back and since then we have also grown and keeping in pace with Cloudera new certifications. We also provide industry class training used by more than 10000 learners across the globe. Check all the products below for more detail.



95 Q & A  
Click Here

Cloudera Hadoop  
& Spark Developer  
CCA175



73 Q & A  
Click Here

Cloudera Hadoop  
BigData Analytics  
CCA159



90+ Solved Scenarios  
Click Here

Cloudera Hadoop  
Administrator  
Certification  
CCA131



79 Q & A  
Click Here

Cloudera Data  
Engineer  
CCP:DE575



Click Here

Package Deal

1. [CCA 175 : Cloudera® Hadoop & Spark Developer : 95 Solved Scenarios](#)
2. [CCA159: Cloudera® Data Analyst Certification : 73 Solved Scenarios](#)
3. [CCA131 : Cloudera Hadoop Administrator Certification : 92 Solved Scenarios](#)
4. [CCP:DE 575 : Cloudera Hadoop Data Engineer : 79 Solved Scenarios](#)
5. [Training : CDH : Cloudera Hadoop Admin Beginner Course-1 : 30 Training Modules](#)
6. [Hadoop Professional Training](#)
7. [HBase Professional Training](#)
8. [Hadoop Package Deal](#)

**About Hortonworks® Training & Certifications:** Hortonworks is one of the leader in providing Big Data solution through their own HDP platform. To check candidate's proficiency or skills for HDP platform they have various certification exams. HDPs most of the exam are Hands-on exam other than HCA (Hortonworks Certified Associate). All the exam aspirant has to solve given tasks on HDP cluster. In each exam there are approx. 10-12 problem scenario would be given and needs to be solved in 2 Hrs. Being an Hands-on exam, these certifications has high value in industry, because it require real hands on experience to solve given scenario. Hence to help you, HadoopExam is providing from scratch how to setup environment to practice scenarios. HadoopExam also provides the complementary videos, where we guide you how to solve problems and setup the environment. Currently we have following certification preparation material available.



74 Solved Scenarios

[Click Here](#)

**HDPCD No-Java  
Developer  
Certification**



65 Solved Scenarios

[Click Here](#)

**HDPCD-Spark  
Developer Exam**



57 Solved Scenarios

[Click Here](#)

**Hortonworks  
HDPCA : Hadoop  
Admin Certification**

1. [HDPCD : Hadoop \(HDP\) No Java Certification : 74 Solved Scenarios](#)
2. [HDPCD-Spark : HDP Certified Developer : 65 Solved Scenarios](#)
3. [HDPCA : HDP Certified Administrator : 57 Solved Scenarios](#)
4. [Hortonworks Certification Package Deal](#)

---

**Data Science & Machine Learning:** Data Science is one of the most demanding field, currently and we are providing following products to become a data scientist from one of the popular organization in the data world EMC



234 Q & A

[Click Here](#)

**EMC Data Scientist  
Associate  
Certification  
E20-007 (EMCDSA)**



108 Q & A

[Click Here](#)

**EMC Data Science  
Specialist (E20-065)**



DS-200

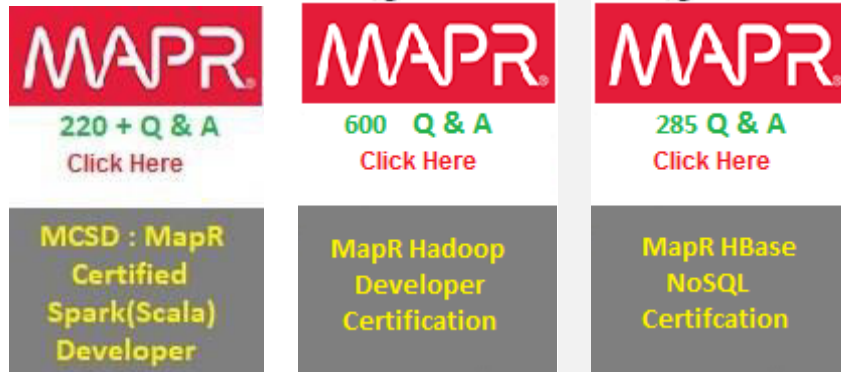
[Click Here](#)

**Cloudera Data  
Science  
Certification DS200**

1. [Data Science Certification EMC® E20-007 \(Data Science Associate\)](#)
2. [EMC® Data Science Specialist \(E20-065\)](#)
3. [Cloudera Data Science DS-200 \(235 Questions + 150 Page Study Notes\) : Retired](#)



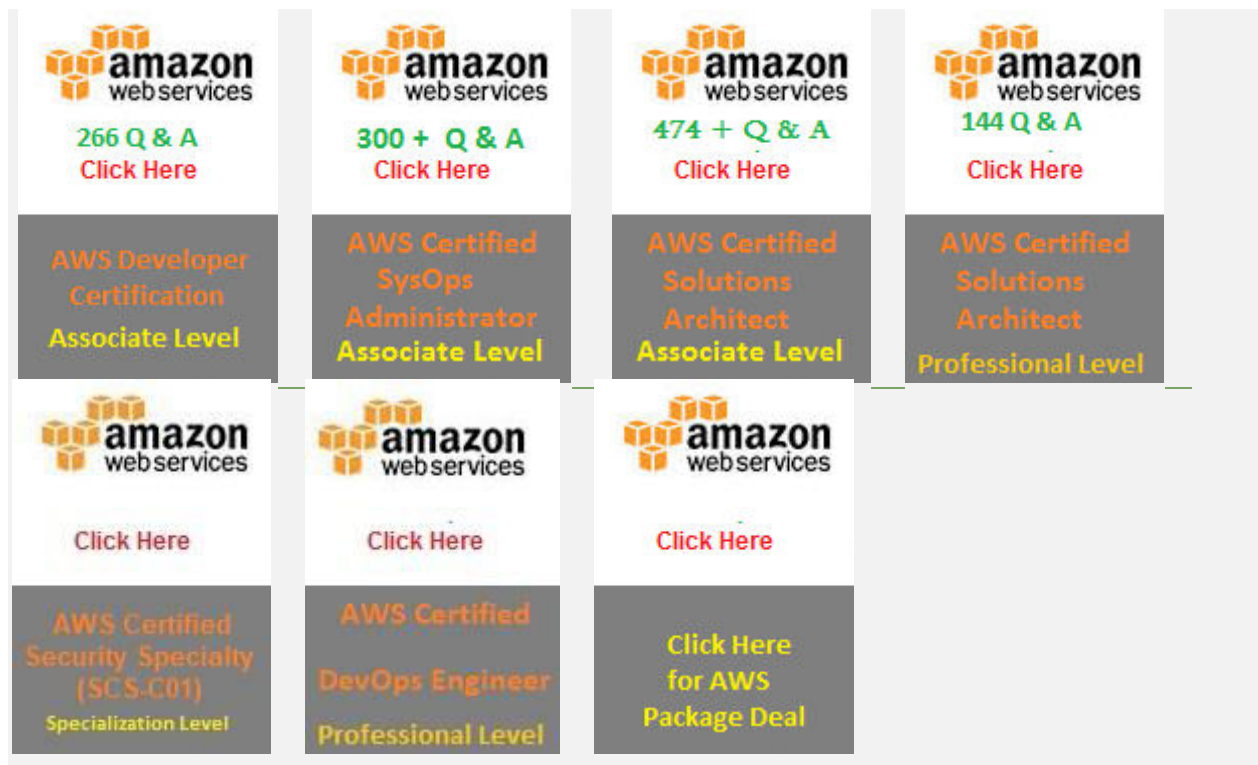
**MapR® Training & Certifications** : MapR is another most popular BigData solution provider based on Hadoop. These are the following certifications, which HadoopExam is providing currently.



1. [MCSD : MapR Spark \(Scala\) Certified Developer](#)
2. [MapR Hadoop Developer Certification](#)
3. [MapR HBase NoSQL Certification](#)
4. [MapR Package Deal](#)

---

**AWS Training & Certifications** : In the Cloud computing world , Amazon is a pioneer and most used Cloud Computing solutions. Currently there are following products are provided bt HadoopExam for the AWS trainings and certifications preparation. We have been providing this matrial since last approx 5 years and many 1000s of learners already using our material to grow in their career.



1. [AWS Developer \(Associate\) Certifications](#)
2. [AWS Solution Architect \(Associate\) Certification Simulator](#)
3. [AWS Solution Architect \(Professional\) Certification Simulator](#)
4. [AWS Sysops Administrator\(Associate\) Certification Simulator](#)
5. [AWS Certified Security Specialty \(SCS-C01\) Certification Simulator](#)
6. [AWS Solution Architect \(Associate\) Certification Training](#)
7. [AWS DevOps Professional Certification Simulator](#)
8. [Book : AWS Solution Architect\(Associate Little Guide\)](#)
9. **Book** : AWS Certified Security Specialty (SCS-C01) : Little Guide (In progress, once released will be available)

- [All Available AWS Products](#)
- [All Available AWS Package](#)

**IBM® BigData Architect** : This is a multiple choice exam conducted by IBM for a BigData Architect. IBM also has Hadoop framework known as BigInsight and they will be asking Question based on BigInsight, however it is very similar to Hadoop only, because they are using Apache Hadoop framework only. As you know, IBM is the oldest and one of the matured software vendor and they have more penetration in the Industry, compare to any other BigData vendor. Hence, certifying yourself as a BigData Architect for IBM, ceratinly have high value in industry.





240 Q & A

[Click Here](#)

IBM C2090-102

Big Data

Architect

- [IBM C2090-102: IBM Big Data Architect : Total 240 Questions : Highest number of Questions : 95% Questions with explanations](#)

---

**DataStax® Apache Cassandra Certification:** This is a multiple choice exam conducted by DataStax for Apache Cassandra. DataStax is one of the leader in providing Apache Cassandra based solutions. Apache Cassandra is one of the most demanding and used NoSQL database across the industry. Cassandra has been used in Finance, HealthCare, Aviation, Retail, e-commerce and many more. It has proved itself with high degree of performance. However, it's a different database and RDBMS principals does not fit with Cassandra. You certainly need to learn Cassandra Data Modeling to design database perfectly and this certification is designed towards this only. And HadoopExam had put lot of effort to create this material to help in clearing this certification exam.



207 Q & A

[Click Here](#)

Professional

Certification

Apache

Cassandra

- [Professional Certification Apache Cassandra\(Datastax\) : Total 207 Questions : Highest number of Questions : 95% Questions with explanations](#)

**SAS®:** One of the most used commercial solutions for analytics, Data science, mathematical and statistical modeling. In analytics world no other solution is close to SAS. Its leader in its field and mostly used across industry. Below are the all products provided by HadoopExam.

|                                                                                                                                         |                                                                                                                                         |                                                                                                                                          |                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <br><b>BASE Training</b><br><a href="#">Click Here</a> | <br><b>490 Q &amp; A</b><br><a href="#">Click Here</a> | <br><b>365 Q &amp; A</b><br><a href="#">Click Here</a> | <br><b>86+ Q &amp; A</b><br><a href="#">Click Here</a> |
| <b>35 Hands On Sessions</b><br><b>20 Module</b>                                                                                         | <b>SAS Base Certification</b><br><b>A00-211</b>                                                                                         | <b>SAS Advance Certification</b><br><b>A00-212</b>                                                                                       | <b>SAS Certified Statistical Business Analyst</b><br><b>A00-240</b>                                                                       |
| <br><b>85 Q &amp; A</b><br><a href="#">Click Here</a>  | <br><a href="#">Click Here</a>                         |                                                                                                                                          |                                                                                                                                           |
| <b>SAS Certified Platform Administrator 9</b><br><b>A00-250</b>                                                                         | <b>SAS Packaged Deal</b>                                                                                                                |                                                                                                                                          |                                                                                                                                           |

1. [SAS Base Certification Professional Training](#)
2. [SAS Base Programming Certification\(A00-211\)](#)
3. [SAS Certified Advanced Programmer for SAS 9 Credential](#)
4. [SAS Certified Statistical Business Analyst Using SAS 9: Regression and Modeling Credential](#)
5. [SAS Certified Platform Administrator 9 \(A00-250\) Certification Practice Questions](#)
6. [SAS Package Deal](#)

---

**HBase Training & Certifications:** HBase is a NoSQL solution based on Hadoop framework. Hence, is very well compitible with the Hadoop based solution. You should certainly learn HBase, if you are wroking in BigData world using HadoopExam. Following are the products provided by HadoopExam for HBase.



1. [HBase professional Training with HandsOn Sessions](#)
2. [MapR HBase certification preparations](#)

---


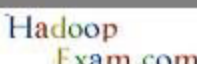

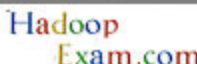

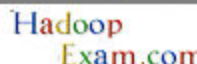

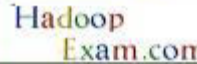
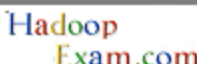


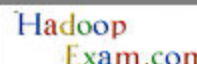
**Microsoft® Azure:** Microsoft Azure is another provider for Cloud computing solutions and also heavily used in the industry. If you are planning to make your career in Cloud computing than you should have very good understanding of the Microsoft Azure. Please find all the products and solution provided by HadoopExam for the Azure.



1. [Microsoft Azure 70-532 Developing Azure Solution Certification](#)
2. [Microsoft Azure 70-533 Implementing Microsoft Azure Infrastructure Solutions](#)

---

**Oracle Cloud , Java and Other Programing Trainings and Certifications:** There is no development without a programming skills. We provide trainings and certification material which will make you developer who can work in well developed IT industry, with the most demanding programming skills. So start learning Java, Scala, Python and complete its certifications as well. Please check all the available products below.

|                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br><b>1Z0-337</b><br><b>IAAS Certified Implementation Specialist</b><br><b>141 Q &amp; A + 18 Page</b><br> | <br><b>Java 8</b><br><b>1Z0-808</b><br><b>Click Here</b><br><b>Java SE 8 Programmer I</b><br><b>154 Q &amp; A</b><br> | <br><b>Java 8</b><br><b>1Z0-809</b><br><b>Click Here</b><br><b>Java SE 8 Programmer II</b><br><b>175 Q &amp; A</b><br> | <br><b>Java 8</b><br><b>1Z0-897</b><br><b>Click Here</b><br><b>Java EE 6 Web Services Developer</b><br><b>154 Q &amp; A</b><br> |
| <b>Upgrade to Oracle Database 12c</b><br><b>Click Here</b><br><b>1Z0-060</b><br><b>200 Q and A</b><br>                                                                                      | <b>Oracle Database 12c: SQL Fundamentals</b><br><b>Click Here</b><br><b>1Z0-061</b><br><b>161 Q and A</b><br>                                                                                         | <br><b>Java 8</b><br><b>Click Here</b><br><b>Training : Core Java 1Z0-808</b><br>                                     |                                                                                                                                                                                                                                                                                                       |

1. [Oracle 1Z0-337 Oracle Oracle Infrastructure as a Service Certified Implementation Specialist](#)
2. [Full length HandsOn Step By Step Training for Java 1z0-808\)](#)
3. [Scala Professional Trainings with HandsOn Session](#)
4. [Python Professional Trainings with HandsOn Session](#)
5. [Java SE-8 Programmer-1 \(1z0-808\) Certification](#)
6. [Java SE-8 Programmer-2 \(1z0-809\)](#)
7. [JAVA EE Web Services Developer \(1z0-897\)](#)
8. [Oracle® 1Z0-060 : Upgrade to Oracle Database 12c Administrator](#)
9. [Questions for Oracle 1Z0-061 : Oracle Database 12c: SQL Fundamentals](#)