Review Questions

1. Which of the following methods will allow an application using an AWS SDK to be authenticated as a principal to access AWS Cloud services? (Choose 2 answers)
2. Create an IAM user and store the user name and password for the user in the application’s configuration.
3. Create an IAM user and store both parts of the access key for the user in the application’s configuration.
4. Run the application on an Amazon EC2 instance with an assigned IAM role.
5. Make all the API calls over an SSL connection.
6. Which of the following are found in an IAM policy? (Choose 2 answers)
7. Service Name
8. Region
9. Action
10. Password
11. Your AWS account administrator left your company today. The administrator had access to the root user and a personal IAM administrator account. With these accounts, he generated other IAM accounts and keys. Which of the following should you do today to protect your AWS infrastructure? (Choose 3 answers)
12. Change the password and add MFA to the root user.
13. Put an IP restriction on the root user.
14. Rotate keys and change passwords for IAM accounts.
15. Delete all IAM accounts.
16. Delete the administrator’s personal IAM account.
17. Relaunch all Amazon EC2 instances with new roles.
18. Which of the following actions can be authorized by IAM? (Choose 2 answers)
19. Installing ASP.NET on a Windows Server
20. Launching an Amazon Linux EC2 instance
21. Querying an Oracle database
22. Adding a message to an Amazon Simple Queue Service (Amazon SQS) queue
23. Which of the following are IAM security features? (Choose 2 answers)
24. Password policies
25. Amazon DynamoDB global secondary indexes
26. MFA
27. Consolidated Billing
28. Which of the following are benefits of using Amazon EC2 roles? (Choose 2 answers)
29. No policies are required.
30. Credentials do not need to be stored on the Amazon EC2 instance.
31. Key rotation is not necessary.
32. Integration with Active Directory is automatic.
33. Which of the following are based on temporary security tokens? (Choose 2 answers)
34. Amazon EC2 roles
35. MFA
36. Root user
37. Federation
38. Your security team is very concerned about the vulnerability of the IAM administrator user accounts (the accounts used to configure all IAM features and accounts). What steps can be taken to lock down these accounts? (Choose 3 answers)
39. Add multi-factor authentication (MFA) to the accounts.
40. Limit logins to a particular U.S. state.
41. Implement a password policy on the AWS account.
42. Apply a source IP address condition to the policy that only grants permissions when the user is on the corporate network.
43. Add a CAPTCHA test to the accounts.
44. You want to grant the individuals on your network team the ability to fully manipulate Amazon EC2 instances. Which of the following accomplish this goal? (Choose 2 answers)
45. Create a new policy allowing EC2:\* actions, and name the policy NetworkTeam.
46. Assign the managed policy, EC2FullAccess, to a group named NetworkTeam, and assign all the team members’ IAM user accounts to that group.
47. Create a new policy that grants EC2:\* actions on all resources, and assign that policy to each individual’s IAM user account on the network team.
48. Create a NetworkTeam IAM group, and have each team member log in to the AWS Management Console using the user name/ password for the group.
49. What is the format of an IAM policy?
50. XML
51. Key/ value pairs
52. JSON
53. Tab-delimited text

질문 검토

1. 다음 중 AWS SDK를 사용하는 응용 프로그램을 인증 할 수있는 방법은 무엇입니까?

AWS Cloud 서비스에 액세스 하시겠습니까? (2 답 선택)

A. IAM 사용자를 만들고 응용 프로그램의 구성에 사용자의 사용자 이름과 암호를 저장합니다.

B. IAM 사용자를 생성하고 응용 프로그램 구성에 사용자의 액세스 키의 두 부분을 모두 저장합니다.

C. IAM 역할이 할당 된 Amazon EC2 인스턴스에서 응용 프로그램을 실행합니다.

SSL 연결을 통해 모든 API 호출을 수행합니다.

2. IAM 정책에서 다음 중 어느 것이 발견됩니까? (2 답 선택)

A. 서비스 이름

B. 지역

C. 행동

D. 암호

3. AWS 계정 관리자가 오늘 귀사를 떠났습니다. 관리자는 루트 사용자와

개인 IAM 관리자 계정. 이 계정으로 그는 다른 IAM 계정과 키를 생성했습니다. 어느

AWS 인프라를 보호하기 위해 오늘해야 할 일은 무엇입니까? (3 답변 선택)

A. 암호를 변경하고 MFA를 루트 사용자에게 추가하십시오.

B. 루트 사용자에게 IP 제한을 설정하십시오.

C. IAM 계정의 키를 변경하고 암호를 변경하십시오.

D. 모든 IAM 계정을 삭제합니다.

E. 관리자의 개인 IAM 계정을 삭제합니다.

F. 새로운 역할을 가진 모든 Amazon EC2 인스턴스를 다시 시작하십시오.

4. IAM이 승인 할 수있는 다음 작업 중 어느 것입니까? (2 답 선택)

A. Windows 서버에 ASP.NET 설치

B. Amazon Linux EC2 인스턴스 실행

C. Oracle 데이터베이스 쿼리

D. Amazon SQS (Amazon Simple Queue Service) 대기열에 메시지 추가

|  |
| --- |
| **2 쪽** |

5. 다음 중 IAM 보안 기능은 무엇입니까? (2 답 선택)

A. 암호 정책

B. Amazon DynamoDB 글로벌 보조 인덱스

C. MFA

D. 통합 청구

6. 다음 중 Amazon EC2 역할을 사용하여 얻을 수있는 이점은 무엇입니까? (2 답 선택)

A. 정책은 필요하지 않습니다.

B. 자격 증명은 Amazon EC2 인스턴스에 저장 될 필요가 없습니다.

C. 키 회전은 필요하지 않습니다.

D. Active Directory와의 통합은 자동으로 수행됩니다.

7. 임시 보안 토큰을 기반으로 다음 중 어느 것입니까? (2 답 선택)

A. Amazon EC2 역할

B. MFA

C. 루트 사용자

D. 연맹

8. 보안 팀은 IAM 관리자 사용자 계정의 취약성에 대해 매우 우려하고 있습니다 (

모든 IAM 기능 및 계정을 구성하는 데 사용되는 계정). 이러한 단계를 잠그기 위해 수행 할 수있는 단계

계정? (3 답변 선택)

A. 여러 요소 인증 (MFA)을 계정에 추가합니다.

B. 특정 미국 주에 로그인 제한.

C. AWS 계정에 암호 정책을 구현하십시오.

D. 사용자가 액세스 할 때만 사용 권한을 부여하는 정책에 원본 IP 주소 조건을 적용합니다.

기업 네트워크.

E. 계정에 CAPTCHA 테스트를 추가하십시오.

9. 네트워크 팀 구성원에게 Amazon EC2 인스턴스를 완벽하게 조작 할 수있는 권한을 부여하려고합니다.

다음 중이 목표를 달성 할 수있는 것은 무엇입니까? (2 답 선택)

|  |
| --- |
| **Page 3** |

A. EC2 : \* 작업을 허용하는 새 정책을 만들고 NetworkTeam 정책의 이름을 지정합니다.

B. 관리되는 정책 인 EC2FullAccess를 NetworkTeam이라는 그룹에 할당하고 모든 팀을 할당합니다

구성원의 IAM 사용자 계정을 해당 그룹에 추가합니다.

C. 모든 리소스에 대해 EC2 : \* 액션을 부여하는 새 정책을 만들고 각 개인의 정책에 할당합니다.

네트워크 팀의 IAM 사용자 계정.

D. NetworkTeam IAM 그룹을 만들고 각 팀 구성원이 AWS Management Console에 로그인하도록합니다.

그룹의 사용자 이름 / 암호를 사용합니다.

10. IAM 정책의 형식은 무엇입니까?

A. XML

B. 키 / 값 쌍

C. JSON

D. 탭으로 구분 된 텍스트

1. B, C. Programmatic access is authenticated with an access key, not with user names/ passwords. IAM roles provide a temporary security token to an application using an SDK.
2. A, C. IAM policies are independent of region, so no region is specified in the policy. IAM policies are about authorization for an already-authenticated principal, so no password is needed.
3. A, C, E. Locking down your root user and all accounts to which the administrator had access is the key here. Deleting all IAM accounts is not necessary, and it would cause great disruption to your operations. Amazon EC2 roles use temporary security tokens, so relaunching Amazon EC2 instances is not necessary.
4. B, D. IAM controls access to AWS resources only. Installing ASP.NET will require Windows operating system authorization, and querying an Oracle database will require Oracle authorization.
5. A, C. Amazon DynamoDB global secondary indexes are a performance feature of Amazon DynamoDB; Consolidated Billing is an accounting feature allowing all bills to roll up under a single account. While both are very valuable features, neither is a security feature.
6. B, C. Amazon EC2 roles must still be assigned a policy. Integration with Active Directory involves integration between Active Directory and IAM via SAML.
7. A, D. Amazon EC2 roles provide a temporary token to applications running on the instance; federation maps policies to identities from other sources via temporary tokens.
8. A, C, D. Neither B nor E are features supported by IAM.
9. B, C. Access requires an appropriate policy associated with a principal. Response A is merely a policy with no principal, and response D is not a principal as IAM groups do not have user names and passwords. Response B is the best solution; response C will also work but it is much harder to manage.
10. C. An IAM policy is a JSON document.

1. B, C. 프로그래밍 방식의 액세스는 사용자 이름 / 암호가 아닌 액세스 키를 사용하여 인증됩니다. IAM 역할은 SDK를 사용하여 응용 프로그램에 임시 보안 토큰을 제공합니다.

2. A, C. IAM 정책은 지역에 독립적이므로 정책에 지역이 지정되지 않습니다. IAM 정책은 이미 인증 된 주체에 대한 권한 부여이므로 암호가 필요하지 않습니다.

3. A, C, E. 루트 사용자와 관리자가 액세스 할 수있는 모든 계정을 잠그는 것이 핵심입니다. 모든 IAM 계정을 삭제할 필요는 없으며 작업을 크게 방해합니다. Amazon EC2 역할은 임시 보안 토큰을 사용하므로 Amazon EC2 인스턴스를 다시 시작하지 않아도됩니다.

4. B, D. IAM은 AWS 리소스에 대한 액세스 만 제어합니다. ASP.NET 설치에는 Windows 운영 체제 인증이 필요하며 Oracle 데이터베이스를 쿼리하려면 Oracle 인증이 필요합니다.

5. A, C. Amazon DynamoDB 글로벌 보조 인덱스는 Amazon DynamoDB의 성능 기능입니다. Consolidated Billing은 단일 계정으로 모든 청구서를 롤업 할 수있는 회계 기능입니다. 둘 다 매우 중요한 기능이지만 보안 기능도 없습니다.

6. B, C. Amazon EC2 역할에는 여전히 정책이 지정되어야합니다. Active Directory와의 통합에는 SAML을 통한 Active Directory와 IAM 간의 통합이 포함됩니다.

7. Amazon EC2 역할은 인스턴스에서 실행되는 응용 프로그램에 임시 토큰을 제공합니다. 연합은 정책을 임시 토큰을 통해 다른 출처의 ID로 매핑합니다.

8. A, C, D B 또는 E는 IAM에서 지원하는 기능이 아닙니다.

9. B, C. 액세스에는 주체와 관련된 적절한 정책이 필요합니다. 응답 A는 단순히 주체가없는 정책 일 뿐이며 IAM 그룹에는 사용자 이름과 암호가 없으므로 응답 D는 주체가 아닙니다. 응답 B가 최상의 솔루션입니다. 응답 C도 작동하지만 관리가 훨씬 어렵습니다.

C. IAM 정책은 JSON 문서입니다.