**1. განმარტეთ ვირტუალური სერვერების სპეციფიკა და მნიშვნელობა.**  
ვირტუალური სერვერები (Virtual Servers) საშუალებას აძლევენ მომხმარებლებს შექმნან და მართონ სერვერები ფიზიკური აპარატურის გარეშე. ისინი განლაგებულია ჰიპერვიზორებზე და უზრუნველყოფენ მოქნილობას, რესურსების ოპტიმიზაციას და მასშტაბირებას.

**2. რა სახის მიკროსერვისებია ხელმისაწვდომი AWS EC2-ში?**  
AWS EC2 მხარს უჭერს Docker კონტეინერებზე დაფუძნებულ მიკროსერვისებს, Lambda ფუნქციებსა და API Gateway-ს, რაც იძლევა ინდივიდუალური სერვისების მარტივად მართვის საშუალებას.

**3. აღწერეთ EC2 ინსტანსების გაშვების და გაჩერების პროცედურები.**  
EC2 ინსტანსები იწყება AWS Management Console-დან ან CLI-დან, სადაც აირჩევთ ინსტანსის ტიპს, AMI-ს, უსაფრთხოების ჯგუფებს და სუბნეტს. გაჩერება ხდება Stop ან Terminate ბრძანებით.

**4. როგორ ხდება ოპერაციული სისტემების არჩევა და კონფიგურაცია?**  
AWS გთავაზობთ სხვადასხვა ოპერაციულ სისტემას (Linux, Windows). მომხმარებელი ირჩევს AMI-ს, რომელიც მოიცავს წინასწარ კონფიგურირებულ OS-ს და საჭიროებას მიხედვით აკონფიგურირებს მას.

**5. რა მექანიზმებია საჭირო SSH/RDP წვდომის ორგანიზებისთვის?**  
საჭიროა უსაფრთხოების ჯგუფების კონფიგურაცია, SSH გასაღებების შექმნა Linux ინსტანსებისთვის და RDP კრედენციების გამოყენება Windows ინსტანსებისთვის.

**1. როგორ მუშაობს Snapshot-ების და AMI-ების შექმნის მექანიზმი?**  
Snapshot-ები ქმნიან მოცულობის სარეზერვო ასლს, ხოლო AMI-ები Snapshot-ზე დაფუძნებული გამოსახულებებია, რომლებიც გამოიყენება ინსტანსების შექმნისთვის.

**2. რა განსხვავებაა სრულ და ინკრემენტულ Snapshot-ებს შორის?**  
სრული Snapshot-ი მოიცავს მთელ მოცულობას, ინკრემენტული კი ინახავს მხოლოდ იმ ცვლილებებს, რაც მოხდა წინა Snapshot-ის შემდეგ.

**3. როგორ ხორციელდება Snapshot-ების რეპლიკაცია რეგიონებს შორის?**  
Snapshot-ების კოპირება შესაძლებელია AWS Management Console ან CLI-დან, რაც უზრუნველყოფს მონაცემების ხელმისაწვდომობას სხვა რეგიონებში.

**4. რა უპირატესობები აქვს AMI-დან ახალი ინსტანსის შექმნას?**  
AMI უზრუნველყოფს წინასწარ კონფიგურირებულ სისტემას, რაც ამარტივებს ინსტანსების სწრაფად და ეფექტურად გაშვებას.

**5. აღწერეთ ბექაპების ავტომატიზაციის შესაძლებლობები.**  
AWS Backup სერვისი საშუალებას იძლევა, ავტომატურად შეიქმნას Snapshot-ები და ბექაპები განსაზღვრული პოლიტიკის მიხედვით.

**1. რა მიზანს ემსახურება სხვადასხვა ქვექსელის შექმნა?**  
ქვექსელები უზრუნველყოფენ ქსელის იზოლაციას, უსაფრთხოებას და რესურსების მართვის სიმარტივეს.

**2. როგორ ხდება IP მისამართების მართვა და სეგმენტაცია?**  
IP მისამართების მართვა ხდება სუბნეტების მეშვეობით, რაც ქსელს ანაწევრებს სეგმენტებად.

**3. რა როლი აქვს Internet Gateway-ს ინფრასტრუქტურაში?**  
Internet Gateway უზრუნველყოფს საჯარო ინტერნეტიდან VPC-ზე წვდომას.

**4. როგორ კონფიგურირდება მარშრუტიზაციის ცხრილები?**  
მარშრუტიზაციის ცხრილები განსაზღვრავენ ქსელის ტრეფიკის მიმართულებას კონკრეტული სუბნეტებისთვის.

**5. რა უსაფრთხოების მექანიზმებია ხელმისაწვდომი VPC-ში?**  
ხელმისაწვდომია უსაფრთხოების ჯგუფები (Security Groups), ქსელის ACL-ები და VPN კავშირები.

**1. როგორ უზრუნველყოფს ბასტიონ ჰოსტი უსაფრთხო წვდომას?**  
ბასტიონ ჰოსტი ფუნქციონირებს როგორც შუამავალი წერტილი, რომელიც უზრუნველყოფს მხოლოდ ავტორიზებულ წვდომას შიდა რესურსებზე.

**2. რა შემთხვევებში გამოიყენება SSH ტუნელირება?**  
SSH ტუნელირება გამოიყენება მონაცემთა უსაფრთხო ტრანსპორტირებისთვის არაუნდარ ქსელებში.

**3. როგორ ხდება წვდომის კონტროლის მექანიზმების დანერგვა?**  
წვდომის კონტროლის მექანიზმები მოიცავს IAM როლებს, უსაფრთხოების ჯგუფებს და NACL-ებს.

**4. რა უსაფრთხოების ზომები უნდა იქნას მიღებული?**  
მონაცემთა დაშიფვრა, უსაფრთხოების ჯგუფების კონფიგურაცია და წვდომის ლოგების მონიტორინგი აუცილებელია.

**5. როგორ ხდება ბასტიონ ჰოსტის მონიტორინგი და აუდიტი?**  
CloudWatch და CloudTrail გამოიყენება ბასტიონ ჰოსტის აქტივობების მონიტორინგისა და აუდიტისთვის.

**1. რა ტიპის NAT სერვისებია ხელმისაწვდომი AWS-ში?**  
AWS-ში ხელმისაწვდომია NAT Gateway და NAT Instance.

**2. როგორ მუშაობს NAT Gateway მარშრუტიზაცია?**  
NAT Gateway საშუალებას აძლევს შიდა ქსელის რესურსებს, ჰქონდეთ ინტერნეტ წვდომა, თუმცა ინარჩუნებენ გაუჩინარობას საჯარო ქსელიდან.

**3. რა უპირატესობები აქვს NAT Gateway-ს NAT Instance-თან შედარებით?**  
NAT Gateway უფრო მაღალი წარმადობითა და ავტომატური მასშტაბირებით გამოირჩევა.

**4. როგორ კონფიგურირდება მაღალი ხელმისაწვდომობა?**  
მაღალი ხელმისაწვდომობა მიიღწევა მრავალ ხელმისაწვდომობის ზონაში NAT Gateway-ის კონფიგურაციით.

**5. რა გავლენა აქვს NAT-ს ქსელის წარმადობაზე?**  
NAT გავლენას ახდენს ქსელის წარმადობაზე, რაც დამოკიდებულია გამოყენებული სერვისის ტიპზე (Gateway ან Instance).

**1. რა მახასიათებლები აქვს S3 სტორიჯის კლასებს?**  
S3 სტორიჯის კლასები განსხვავდებიან შესრულების, ღირებულებისა და წვდომის სიხშირის მიხედვით (Standard, Intelligent-Tiering, Glacier და სხვ.).

**2. როგორ მუშაობს S3 ვერსიონირების მექანიზმი?**  
S3 ვერსიონირების ფუნქცია ინახავს ფაილების ყველა ვერსიას, რაც ხელს უწყობს მონაცემთა აღდგენას შეცდომის შემთხვევაში.

**3. რა შესაძლებლობებია ხელმისაწვდომი ფაილების მართვისთვის?**  
ხელმისაწვდომია ფაილების ატვირთვა, გადმოწერა, წაშლა და არქივირება.

**4. როგორ ხორციელდება S3 ბაკეტებზე წვდომის კონტროლი?**  
IAM პოლიტიკები, ბაკეტის ACL-ები და S3 Block Public Access ფუნქცია გამოიყენება.

**5. როგორ შეიძლება S3-ის პროგრამული მართვა EC2-დან?**  
SDK-ებისა და CLI-ის გამოყენებით S3-ს EC2-დან პროგრამულად მართვა შესაძლებელია.

**1. რა კონფიგურაცია სჭირდება S3-ს ვებ ჰოსტინგისთვის?**  
საჭიროა ბაკეტის შექმნა, სტატიკური ვებსაიტის ჩართვა და ფაილების ატვირთვა.

**2. როგორ ხდება დომეინების მიბმა S3 ვებსაიტებზე?**  
დომეინების მიბმა ხორციელდება Route 53-ის ან სხვა DNS პროვაიდერის გამოყენებით.

**3. როგორ კონფიგურირდება HTTPS წვდომა?**  
CloudFront დისტრიბუციის და SSL სერთიფიკატის გამოყენებით.

**4. რა სერვისებთან ინტეგრაცია არის შესაძლებელი?**  
S3 ინტეგრირდება Lambda-სთან, CloudFront-თან, და RDS-თან.

**5. როგორ ხდება კონტენტის განახლების ავტომატიზაცია?**  
AWS CLI ან SDK-ის გამოყენებით ფაილების ატვირთვის ავტომატიზაცია.

**1. როგორ ხდება RDS ინსტანსის ტიპის შერჩევა?**  
მომხმარებელი ირჩევს ინსტანსის ტიპს შესრულების, მასშტაბისა და ფასის მიხედვით.

**2. რა ოფციებია ხელმისაწვდომი მაღალი ხელმისაწვდომობისთვის?**  
Multi-AZ Deployment და Read Replica ფუნქციები.

**3. როგორ კონფიგურირდება მონაცემთა ბაზის რეპლიკაცია?**  
Replica-ების შექმნა ხდება AWS Management Console ან CLI-დან.

**4. რა უსაფრთხოების მექანიზმებია ხელმისაწვდომი?**  
VPC, IAM პოლიტიკები, და მონაცემთა დაშიფვრა.

**5. როგორ ხდება მონაცემთა ბაზის მონიტორინგი და ოპტიმიზაცია?**  
CloudWatch Metrics და Performance Insights გამოიყენება მონიტორინგისთვის.

**1. როგორ მუშაობს IAM როლების იერარქია?**  
IAM როლები განსაზღვრავენ რესურსებზე წვდომის უფლებებს და პასუხისმგებლობებს.

**2. რა განსხვავებაა Resource და Identity პოლისებს შორის?**  
Resource პოლიტიკა კონკრეტულ რესურსებზე ვრცელდება, Identity პოლიტიკა კი მომხმარებელზე ან როლზე.

**3. როგორ ხდება წვდომების აუდიტი და მონიტორინგი?**  
CloudTrail და Access Analyzer გამოიყენება წვდომის ლოგებისა და პოლიტიკების მონიტორინგისთვის.

**4. რა საუკეთესო პრაქტიკებია წვდომების მართვისთვის?**  
მინიმალური ნებართვები, რეგულარული აუდიტი და MFA-ის ჩართვა.

**5. როგორ კონფიგურირდება კროს-აქაუნთ წვდომები?**  
Role Trust Policies-ის კონფიგურაციით.