WEBVTT

00:00:00.000 --> 00:00:07.360

Қайырлы күн, құрметті студенттер. Біз Practice Test сұрағын талдауды бастаймыз.

00:00:07.360 --> 00:00:15.600

Сұрақтың шарты бойынша, компания жергілікті дата-центрде сақтайтын құпия деректердің белгілі бір көлемін жасайды.

00:00:15.600 --> 00:00:25.120

Сақтық көшірме шешімі ретінде компания бұл деректерді Amazon S3 bucket-інде сақтағысы келеді.

00:00:25.120 --> 00:00:38.200

Кейбір ішкі компания қауіпсіздік талаптарына сай деректерді S3 жүйесіне жібермес бұрын шифрлау талап етіледі.

00:00:38.200 --> 00:00:47.320

Сонымен қатар, компания шифрлау кілттерін дербес басқаруы және жаңартуы керек.

00:00:47.320 --> 00:00:56.440

Сондай-ақ, бұл кілттер компанияның бақылауында болуы керек.

00:00:56.440 --> 00:01:03.040

Ұсынылған әдістердің қайсысы бұған қол жеткізуге көмектеседі?

00:01:03.040 --> 00:01:06.160

Бұл слайдта сіз ұсынылған жауап нұсқаларын көре аласыз.

00:01:06.160 --> 00:01:09.280

Сондай-ақ, 3 және 5 дұрыс екенін көреміз.

00:01:09.280 --> 00:01:12.800

Сұрақтарды талдауды бастамас бұрын, теорияны еске түсірейік.

00:01:12.800 --> 00:01:22.640

Теорияны біле отырып, S3 сервисінде шифрлауға қатысты кез келген сұраққа жауап беру оңайырақ болады.

00:01:22.640 --> 00:01:27.520

Біз білетіндей, шифрлаудың екі түрі бар.

00:01:27.520 --> 00:01:36.640

Бұл in-transit шифрлау, деректер бір жерден екінші жерге тасымалданған кезде және at rest, яғни деректер сақталған кезде.

00:01:36.640 --> 00:01:47.960

Егер S3 туралы айтатын болсақ, in-transit S3-ке деректерді тасымалдау және деректерді жүктеу процесін білдіреді.

00:01:47.960 --> 00:02:00.680

Ал at rest кезінде десек, деректер AWS дата-центрлеріндегі S3 сервисінде болғанда айтамыз.

00:02:00.680 --> 00:02:12.440

Біз in-transit шифрлауды айтқанда, SSL кілтін немесе клиенттік шифрлауды пайдалануды түсінеміз.

00:02:12.440 --> 00:02:26.800

Ең танымал және айқын мысал - браузерде, веб-сайтты ашқанда, қосылым HTTPS арқылы екенін көрсеңіз, бұл қауіпсіз қосылым.

00:02:26.800 --> 00:02:41.400

Сонымен, бұл жағдайда арнайы SSL сертификаты қосылады, ол in-transit сізден веб-сайтқа деректерді тасымалдауды шифрлауға көмектеседі.

00:02:41.400 --> 00:02:55.560

S3 сервисіне қатысты at rest туралы айтқанда, екі түбегейлі әртүрлі топ бар, олар Server-Side Encryption және Client-Side Encryption.

00:02:55.560 --> 00:03:09.200

Server-Side Encryption деген кезде, біз деректерді S3-ге тасымалдаймыз, содан кейін S3 өз жағындағы деректерді шифрлайды және оны қатқыл дискілерге сақтайды.

00:03:09.200 --> 00:03:34.440

Client-Side Encryption туралы айтқанда, бұл деректер S3-ке тасымалданбас бұрын кейбір кілттермен шифрланғанын және S3 шифрланған файлды алатынын білдіреді, оны қайтадан шифрлаудың қажеті жоқ және ол бұл файлды сол күйінде қатқыл дискіге сақтайды.

00:03:34.440 --> 00:03:53.720

Егер кері процесс туралы айтатын болсақ, Server-Side Encryption жағдайында S3 шифрлау кілттерін пайдаланып, файлдарды өз жағындағы қатқыл дискілерден алады, осы файлдардың шифрын шешеді және бұл деректерді сізге жібереді.

00:03:53.720 --> 00:04:09.160

Егер Client-Side Encryption десек, S3-тен файлды жүктеп алу кезінде келесі жағдай орын алады: S3 қатқыл дискілерден деректерді шығарып алады және оның шифрін шешпей сізге сол пішінде жібереді.

00:04:09.160 --> 00:04:21.640

Сіз шифрланған файлды сол тасымалдаған пішінде аласыз және шифрлау кілттерін пайдалана отырып, бұл файлдың шифрын шешесіз және оны пайдалана бересіз.

00:04:21.640 --> 00:04:25.120

Шифрды шешу процесінің өзі сіздің жағыңызда болады.

00:04:25.120 --> 00:04:46.600

Осылайша дұрыс жауап нұсқасы AWS KMS сервисімен Client-Side Encryption пайдалану деп айтамыз, ал екінші нұсқа да бізде, яғни клиентте, сақталған мастер кілтті пайдаланатын Client-SideEncryption болып табылады.

00:04:46.600 --> 00:05:03.080

Қалған нұсқалар туралы айтатын болсақ, олар дұрыс емес, өйткені екі дұрыс емес нұсқада Server-Side Encryption бар, бұл сұрақтың шартына қайшы келеді.

00:05:03.080 --> 00:05:10.760

Сондай-ақ, басқа нұсқа бар: Set-up Client-Side encryption with Amazon S3 managed encryption keys.

00:05:10.760 --> 00:05:13.120

Бұл нұсқа теориялық тұрғыдан мүмкін емес.

00:05:13.120 --> 00:05:34.360

Бұл жерде managed encryption key айтамыз, ол бізге клиент ретінде қол жетімді емес, оны S3 басқарады, деректерімізді шифрлау үшін пайдаланылады және біз оған қол жеткізе алмаймыз, оны қандай да бір жолмен өзгерте алмаймыз немесе жаңарта алмаймыз.

00:05:34.360 --> 00:05:49.440

Ал Client-Side encryption with S3 managed encryption key нұсқасының өзі қисынсыз, яғни біз оған жеткенге дейін шифрлау үшін бұл кілттерді шығарудың ешқандай жолы жоқ, ал мұнда Client-Side Encryption дейді.

00:05:49.440 --> 00:05:52.040

Сондықтан, бұл нұсқаның өзі дұрыс емес.

00:05:52.040 --> 00:05:57.440

Осымен біз Practice Test сұрағын талдадық.

00:05:57.440 --> 00:06:00.440

Назарларыңызға рахмет.