WEBVTT

00:00:00.000 --> 00:00:02.520

Қайырлы күн, құрметті студенттер!

00:00:02.520 --> 00:00:07.400

Барлықтарыңызды келесі зертханалық шолу сессиясында көргеніме қуаныштымын.

00:00:07.400 --> 00:00:14.840

Бүгінгі зертханалық жұмыстың тақырыбы - біздің бизнес жағдайымызға, яғни кафеге арналған желіні орнату.

00:00:14.840 --> 00:00:29.080

Бұл зертханалық жұмыс Challenge Lab болып табылады, яғни өте аз нұсқаулар беріледі және өз бетімізше шешімін табуымыз керек.

00:00:29.080 --> 00:00:38.040

Сондай-ақ, зертханалық жұмыстың өзі өте ауқымды екенін атап өткім келеді, бұл сізге ұнайды және оны жасауға қызығушылық танытады деп сенемін.

00:00:38.040 --> 00:00:42.160

Ендеше, бастайық.

00:00:42.160 --> 00:00:48.320

Зертханалық жұмысымызды AWS Academy-дегі Cloud Architecting курсының негізгі парақшасынан бастаймыз.

00:00:48.320 --> 00:00:53.120

Сол жақтағы шарлау мәзірін пайдаланып, модульге өту керек.

00:00:53.120 --> 00:01:03.760

Мұнда бізді алтыншы модуль қызықтырады, атап айтқанда Challenge Lab Creating VPC Networking Environment for the Cafe сілтемесі.

00:01:03.760 --> 00:01:15.720

Зертхананың негізгі парақшасына кіргеннен кейін,Terminal терезесі кедергі жасамайтындай етіп жасырып, зертхана тақырыбын қайта тексеру керек.

00:01:15.720 --> 00:01:21.040

Барлығын орындағаннан кейін, бизнес кейсімізге көшеміз.

00:01:21.040 --> 00:01:33.480

Оған сәйкес, София мен Никхил жақында ғана AWS бұлтындағы архитектураны жақсартты және дерекқордыAmazon RDS managed service-тегі EC2 инстансына көшірді.

00:01:33.480 --> 00:01:54.440

Бұл бүкіл инфрақұрылымның өнімділігін жақсартты, дерекқорды жүргізуге байланысты әкімшілік жұмыстардан босатты, сонымен қатар олар дерекқор ресурстарын public subnet-тен private subnet-ке ауыстырып, оны одан да қауіпсіз етті.

00:01:54.440 --> 00:01:56.640

Жақында олар Матеомен кездесті.

00:01:56.640 --> 00:02:10.000

Матео - AWS жүйесіндегі жүйелік әкімші және ол біздің кейіпкерлеріміздің жаңартуларын тыңдап, архитектураны одан әрі жақсартуға кеңес берді.

00:02:10.000 --> 00:02:24.280

Ол VPC-ді дұрыс орнатуды, оның барлық қажетті құрамдастарын жасауды, сонымен қатар әкімшілік құқықтарға қашықтан қол жеткізу үшін барлық қажетті ресурстарды құруды ұсынды.

00:02:24.280 --> 00:02:33.720

Сондай-ақ, бұл шешім дұрыс жұмыс істейтініне және шабуылдардың болмауына көз жеткізу үшін қауіпсіздіктің қосымша қабаттарын қосу қажет болады.

00:02:33.720 --> 00:02:42.840

Зертханалық жұмыстың аясында біз VPC және оның негізгі компоненттерін құруды үйренеміз.

00:02:42.840 --> 00:02:52.000

Әрі қарай, private subnet-тегі ресурстарға қауіпсіз, қашықтан қосылуға мүмкіндік беретін ресурстарды қалай жасау керектігін үйренеміз.

00:02:52.000 --> 00:03:05.280

Сондай-ақ, VPC периметрін одан әрі қорғау үшін қосымша қауіпсіздік деңгейлерін баптаймыз.

00:03:05.280 --> 00:03:15.520

Зертханалық жұмысты аяқтағаннан кейін, AWS бұлтындағы архитектураның қандай болатынын слайдтан көре аласыз.

00:03:15.520 --> 00:03:24.040

Бұл зертханалық жұмысты орындау үшін 90 минут ұсынылады.

00:03:24.040 --> 00:03:32.480

Егер бұл уақыт жеткіліксіз болса, End lab батырмасын баспай-ақ, Start lab батырмасын басып, есептегішті басына келтіруге болады.

00:03:32.480 --> 00:03:48.080

Сондай-ақ, зертханалық жұмыстар үшін арнайы әзірленген уақытша AWS аккаунты жасалып жатқанын және зертханалық жұмыстарға қатысы жоқ барлық сервистер мен құрамдас бөліктердің қолжетімсіз болуы мүмкін екенін еске саламыз.

00:03:48.080 --> 00:03:54.760

Зертханалық жұмыста қолданылатын барлық сервистер мен компоненттердің қолжетімді болуына кепілдік беріледі.

00:03:54.760 --> 00:04:06.800

Зертханалық жұмысты бастау үшін Start lab батырмасын басып, зертханалық жұмысты бастайтынымызды растап, уақытша AWS аккаунты жасалуы аяқталғанша күту керек.

00:04:06.800 --> 00:04:09.360

Сіз оның жұмыс істеуге дайын күйін көресіз.

00:04:09.360 --> 00:04:20.640

Осыдан кейін уақытша AWS аккаунтына ауысып, зертханалық жұмысты орындауды бастау үшін AWS батырмасын басуға болады.

00:04:20.640 --> 00:04:38.200

Біз тапсырмалардың бірінші блогына жеттік және бизнес-кейстің аясында VPC ішінде bastion host-тан бастап, subnet-ке дейінгі әлі жасалмаған барлық қажетті компоненттерді жасау керек.

00:04:38.200 --> 00:04:43.560

Әрі қарай, bastion host-ының Интернеттен қол жетімді екеніне көз жеткізуіміз керек.

00:04:43.560 --> 00:05:01.280

Осыдан кейін private subnet-тен Интернетке қауіпсіз қосыла алатындай, бірақ private subnet-тегі ресурстарға қолжетімділік тек public subnet-тегі EC2 инстансы арқылы болатындай етіп барлық қажетті қадамдарды жасаймыз.

00:05:01.280 --> 00:05:03.720

Біздің жағдайда, бұл - bastion host.

00:05:03.720 --> 00:05:04.960

Ендеше, бастайық.

00:05:04.960 --> 00:05:05.960

Бірінші тапсырма.

00:05:05.960 --> 00:05:09.840

Бірінші тапсырманың аясында public subnet құруымыз керек.

00:05:09.840 --> 00:05:21.880

Уақытша AWS аккаунтындағы бар VPC тізімінде Lab VPC деп аталатын VPC жасалғанын ескеріңіз.

00:05:21.880 --> 00:05:24.000

Оны кейін пайдаланамыз.

00:05:24.000 --> 00:05:25.000

Келесі қадам.

00:05:25.000 --> 00:05:27.520

Бізге public subnet құру керек.

00:05:27.520 --> 00:05:36.160

Ол үшін subnet-тер тізіміне өтіп, жаңа subnet құру үшін тиісті батырманы басамыз.

00:05:36.160 --> 00:05:45.040

Name ретінде Public subnet көрсетеміз, VPC ретінде Lab VPC таңдаймыз, Availability zone ретінде а-ға аяқталатынды таңдауымыз керек.

00:05:45.040 --> 00:05:55.160

Уақытша AWS аккаунты North Virginia аймағында жасалған болса, Availability zone ретінде us-east-1a таңдау керек.

00:05:55.160 --> 00:06:01.040

CIDR block ретінде келесі мәнді көрсетеміз және subnet жасаймыз.

00:06:01.040 --> 00:06:11.680

Содан кейін Internet gateway жасап, оны VPC-ге байланыстыруымыз керек.

00:06:11.680 --> 00:06:25.160

Келесі қадам - ​​public subnet-тің route table-ін баптау, осылайша интернет трафик target ретінде Internet gateway-ді пайдаланады.

00:06:25.160 --> 00:06:37.520

Осыдан кейін кастомдық route table жасалған болса, route table-ді public subnet-ке байланыстыру қажет.

00:06:37.520 --> 00:06:57.240

Егер әдепкі route table қолданып, өзгерткен болсақ, онда байланыстырудың қажеті жоқ, ол VPC ішіндегі барлық subnet-терге автоматты түрде байланыстырылған, мұнда біз кастомдық route table-ді нақты көрсетпедік.

00:06:57.240 --> 00:07:03.640

Екінші тапсырмада bastion host жасауымыз керек.

00:07:03.640 --> 00:07:13.920

Bastion host-ты public subnet-те жасаймыз, бұл SSH бойынша Интернет арқылы қосылатын EC2 инстансы.

00:07:13.920 --> 00:07:19.520

Осы EC2 инстансын жасау кезінде қандай параметрлерді көрсету керек екенін қарастырайық.

00:07:19.520 --> 00:07:26.720

Операциялық жүйе ретінде Amazon Linux, Amazon Linux 2 AMI (HVM) нұсқасын қолданамыз.

00:07:26.720 --> 00:07:29.360

Instance Type - t2.micro болуы керек.

00:07:29.360 --> 00:07:37.540

Әрі қарай, Auto-assign public IP параметрінде жалпы IP мекенжайы тағайындалмауы үшін құсбелгіні алып тастау керек.

00:07:37.540 --> 00:07:45.880

Бұл не үшін қажет екенін қазір қарастырамыз және келесі қадамда қосымша талдаймыз.

00:07:45.880 --> 00:08:11.600

Name ретінде Bastion host көрсетуіңіз керек, сонымен қатар Bastion host SG атымен Security тобын жасауыңыз керек және оны тек 22 портта Inbound трафикке рұқсат беру үшін пайдалануыңыз керек, яғни бұл тек біздің IP мекенжайымыз үшін inbound трафикке рұқсат беретін SSH трафигі.

00:08:11.600 --> 00:08:17.560

Private key ретінде vockey қолданамыз.

00:08:17.560 --> 00:08:23.520

Енді үшінші тапсырмада Elastic IP address жасауымыз керек.

00:08:23.520 --> 00:08:35.200

Естеріңізде болса, Bastion host компанияның барлық қызметкерлері қашықтан қосылатын инстанс және ол жалпыға ортақ кіру нүктесі болып табылады.

00:08:35.200 --> 00:08:40.600

Сондықтан оның IP мекенжайы барлығына белгілі және өзгермеуі өте маңызды.

00:08:40.600 --> 00:08:59.960

Егер біз инстанс үшін жалпыға ортақ IP мекенжайын жасасақ, онда bastion host белгілі бір себептермен қайта жасалғанда, оның жалпы IP мекенжайы өзгеруі мүмкін және біз оны алдыңғысына қайтара алмаймыз.

00:08:59.960 --> 00:09:11.720

Осылайша, Bastion host ескі IP мекенжайы жазылған қызметкерлер бұлттағы инфрақұрылымымызға қосыла алмайды.

00:09:11.720 --> 00:09:19.840

Сондықтан, дұрыс шешім - жалпыға ортақ IP мекенжайын тұрақты ету және ол үшін Elastic IP address жасаймыз.

00:09:19.840 --> 00:09:27.180

Оны жасағаннан кейін, оны bastion host-қа байланыстыруымыз керек.

00:09:27.180 --> 00:09:32.240

Төртінші тапсырмада bastion host-ымен байланысты тексеруіміз керек.

00:09:32.240 --> 00:09:46.960

Мұны істеу үшін зертханалық жұмыстың парақшасында Details батырмасын басып, ашылмалы тізімнен AWS жанындағы Show батырмасын басыңыз.

00:09:46.960 --> 00:09:52.000

Мұнда жеке кілтті екі нұсқада жүктеп алу мүмкіндігі бар.

00:09:52.000 --> 00:09:59.040

Егер Windows операционды жүйесі болса, PPK-мен аяқталатын кілтті жүктеп алу керек.

00:09:59.040 --> 00:10:10.400

Егер сіз Linux немесе macOS операционды жүйесімен жұмыс істеп жатсаңыз, бұл жағдайда PEM кеңейтімі бар кілтті жүктеп алуыңыз керек.

00:10:10.400 --> 00:10:17.360

Жүктеп алғаннан кейін, осы терезені жауып, bastion host-ына қосылуға болады.

00:10:17.360 --> 00:10:32.120

Біз зертханалық жұмыста және Демо сессияларымызда қашықтағы EC2 инстансына қосылу жолын бірнеше рет жасадық, сондықтан бұл жерде егжей-тегжейлі тоқталмаймыз.

00:10:32.120 --> 00:10:39.440

Бесінші тапсырмада private subnet жасау керек.

00:10:39.440 --> 00:10:58.120

Private subnet параметрлері үшін Name ретінде Private subnet көрсетеміз, Availability zone ретінде Public subnet үшін көрсетілген availability zone көрсетеміз, CIDR блогы ретінде келесі мәнді көрсетеміз және осымен private subnet жасаймыз.

00:10:58.120 --> 00:11:06.400

Бірақ private subnet-тен Интернетке қауіпсіз кіру мүмкіндігін қамтамасыз ету үшін NAT gateway жасау керек.

00:11:06.400 --> 00:11:27.680

NAT gateway public subnet-те жасалады және NAT gateway-мен қатар Elastic IP address жасау керек екенін еске саламын. Осыдан кейін private subnet-тің route table-де routing rule қосу керек, ол интернет-трафикті NAT gateway-ге бағыттайды.

00:11:27.680 --> 00:11:37.920

Зертханалық жұмыстың аясында private route table деп аталатын route table жасауымыз керек.

00:11:37.920 --> 00:11:55.200

Бұл өте маңызды, өйткені біздің орындалған жұмысымызды автоматты түрде бағалау кезінде бұл да ескерілуі мүмкін және сіздің ұпайларыңызға әсер етуі мүмкін, сондықтан ресурстарымыз үшін енгізуіміз керек мәнді қатаң сақтау қажет.

00:12:07.200 --> 00:12:24.560

Жетінші тапсырмада private subnet-тегі EC2 инстансына bastion host-ына байланысты тексеру үшін private subnet-те EC2 инстансын жасау керек болады.

00:12:24.560 --> 00:12:55.080

Қандай параметрлерді енгізу керек екенін көрейік, AMI ретінде Amazon Linux2 AMI (HVM), Instance Type ретінде t2.micro, атау ретінде Private instance және Security тобында bastion host security group үшін тек 22 порты бойынша кіріс трафикті белгілейміз.

00:12:55.080 --> 00:13:07.480

Сондай-ақ, private subnet-тегі инстанс үшін жаңа private key жасайтынымызды ескеріңіз.

00:13:07.480 --> 00:13:12.080

Оны vockey2 деп атаймыз.

00:13:12.080 --> 00:13:18.640

Сегізінші тапсырмаға жеттік және бұл жасаған барлық қадамдарды сынаудың алдындағы соңғы қадам.

00:13:18.640 --> 00:13:35.240

Мұнда bastion host-та private кілтті сақтамай, bastion host-қа, сондай-ақ bastion host-тан private subnet-тегі EC2 инстансына қосылу мүмкіндігін баптауымыз керек.

00:13:35.240 --> 00:13:49.960

Басқаша айтқанда, Интернет арқылы SSH протоколы бойынша кез келген қашықтағы серверге қосылғанда, біз жеке кілтті компьютерде жергілікті түрде сақтаймыз.

00:13:49.960 --> 00:14:05.400

PuTTY арқылы қосылған кезде, бағдарлама параметрлерінде бұл кілттің қайда орналасқанын көрсетеміз және қосылу кезінде жалпы IP мекенжайын көрсетеміз және кілтпен бірге осы инстансқа сәтті қосыламыз.

00:14:05.400 --> 00:14:21.720

Енді келесі қадам, осы инстансқа қосылған кезде, біздің жағдайда бұл bastion host, SSH арқылы басқа EC2 инстансына қайта қосылуымыз керек, бірақ бұл EC2 инстансы private subnet-те орналасқан.

00:14:21.720 --> 00:14:32.240

Сондықтан, мұны істеу үшін екінші EC2 инстансына қосылу үшін bastion host-ында жеке кілт болуы керек.

00:14:32.240 --> 00:14:46.400

Бұл қауіпті, өйткені бір пайдаланушы арқылы bastion host-қа қосылатын барлық пайдаланушылар олар көрмеуі тиіс кілттерді көруі мүмкін.

00:14:46.400 --> 00:14:55.960

Сондықтан бұл қауіпсіздік тұрғысынан ең жақсы тәсіл емес, бірақ SSH passthrough деп аталатын дайын шешім бар.

00:14:55.960 --> 00:15:21.400

Идея мынада: сіз барлық қажетті кілттерді жергілікті түрде сақтайсыз және SSH арқылы бірнеше инстансқа дәйекті түрде қосылсаңыз, бұл кілттер сіз қосылып жатқан инстанстан ізделмейді, олар алғаш SSH қосылымы болған жергілікті компьютерден алынады.

00:15:21.400 --> 00:15:25.720

Бұл үшін не істеу керек?

00:15:25.720 --> 00:15:33.320

Windows операциялық жүйесінің пайдаланушылары үшін сілтеме бойынша өтіп, Pageant бағдарламасын жүктеп алу керек.

00:15:33.320 --> 00:15:38.640

Бұл бағдарламаны да PuTTY бағдарламасын жасаған топ әзірлеген.

00:15:38.640 --> 00:15:43.760

Оны жүктеп алғаннан кейін орнатып, іске қосуымыз керек.

00:15:43.760 --> 00:15:59.960

Оны іске қосқаннан кейін, өте қарапайым интерфейс болады және екі кілтті Bastion Host-тан vockey және private subnet-тен vockey2 осы бағдарламаға қосу керек.

00:15:59.960 --> 00:16:07.400

Жеке кілттеріңізде .PPK кеңейтімі болуы керек екенін ескеріңіз.

00:16:07.400 --> 00:16:25.320

Әрі қарай, PuTTY арқылы қосылу кезінде қосымша параметрлерді енгізу қажет болады, атап айтқанда Connection - SSH - Auth жолы арқылы өтіп, Allow agent forwarding үшін құсбелгі қойыңыз.

00:16:25.320 --> 00:16:37.040

Сондай-ақ, сол бөлімдегі Credentials бөлімін, атап айтқанда, Private key for authentication өрісін толтыруды ұмытпаңыз.

00:16:37.040 --> 00:16:41.480

Мұнда bastion host-ына қосылу үшін private key таңдауымыз керек.

00:16:41.480 --> 00:16:45.680

Біздің жағдайда, бұл - vockey.

00:16:45.680 --> 00:16:58.320

Оны жасағаннан кейін, біздің bastion host-ымыздың жалпы IP мекенжайын пайдаланып, қосылып көреміз.

00:16:58.320 --> 00:17:08.120

MacOS немесе Linux операциялық жүйесі бар пайдаланушылар үшін тапсырмада көретін келесі командаларды ретімен енгізу керек.

00:17:08.120 --> 00:17:28.880

Идеясы бірдей, сіз кілттерді параметрлердің белгілі бір жерінде сақтайсыз, содан кейін қосымша белгімен қосылған кезде bastion host-ына SSH қосылымын жасайсыз.

00:17:28.880 --> 00:17:32.960

Енді bastion host-ына қосылуымыз керек.

00:17:32.960 --> 00:17:43.360

Қосылғаннан кейін, bastion host-ынан private subnet-тегі EC2 инстансына қосылуымыз керек.

00:17:43.360 --> 00:17:48.120

Оны қалай жасау керектігін білесіз, сондықтан мұнда көп тоқталмаймын.

00:17:48.120 --> 00:17:55.760

Private subnet-тегі EC2 инстансына сәтті қосылғаннан кейін, осы инстанстың Интернетке кіру мүмкіндігі бар-жоғын тексерейік.

00:17:55.760 --> 00:18:18.080

Мұны істеу үшін қарапайым ping командасын және барлық сегіздіктері бар IP мекенжайын енгізуге болады, егер пакеттер алмасуын көрсеңіз және бұл пакеттер алмасу сәтті болса, бұл инстанстың Интернетке кіру мүмкіндігі бар және барлық параметрлерді дұрыс енгіздік дегенді білдіреді.

00:18:18.080 --> 00:18:30.360

Біз зертханалық жұмысымыздың екінші блогына жеттік және мұнда қауіпсіздіктің қосымша деңгейлерін жасаймыз.

00:18:30.360 --> 00:18:56.440

Бизнес-кейсімізге сәйкес, София мен Никхил бұлттық архитектурадағы жаңартуларын досы Матеомен бөлісті, ол барлық жаңартуларды тыңдағаннан кейін, қосымша AWS бұлтындағы IT архитектурасын одан әрі қорғау үшін Network ACL пайдалануды ұсынды. Енді оны жасайтын боламыз.

00:18:56.440 --> 00:19:00.120

Бірінші кезекте Network ACL жасау керек.

00:19:00.120 --> 00:19:12.800

Бұл Network ACL кастомдық болып табылады, біз әдепкі Network ACL барлық кіріс және шығыс трафикке рұқсат беретінін және әдепкі бойынша subnet-терге байланыстыратынын есте ұстаймыз.

00:19:12.800 --> 00:19:28.440

Custom Network ACL жасаған жағдайда, әдепкі бойынша кіріс және шығыс қатынас жабылады және кіруге рұқсат беру үшін қосымша ережелер жасау керек.

00:19:28.440 --> 00:19:42.680

Бізге Custom Network ACL-ді Lab Network ACL деп атап, оны private subnet-ке байланыстыру керек.

00:19:42.680 --> 00:19:57.240

Әрі қарай, осы Custom subnet үшін біз барлық кіріс және шығыс трафикке рұқсат беруіміз керек, содан кейін оны 11-ші тапсырмада сынаймыз.

00:19:57.240 --> 00:20:08.960

Оны тексеру үшін public subnet-те келесі параметрлері бар сынақ EC2 инстансын жасау керек.

00:20:08.960 --> 00:20:29.040

AMI ретінде Amazon Linux 2 AMI (HVM), Instance Type ретінде t2.micro болады, атауы Test Instance болады және осы инстанстың Security тобында барлық кіріс ICMP IPv4 трафигіне рұқсат беруіміз керек.

00:20:29.040 --> 00:20:37.440

Бұл - команда жолында ping командасын іске қосқаннан кейін келетін трафик.

00:20:37.440 --> 00:21:13.280

Осы сынақ инстансының жеке IP мекенжайын ол жасалған бойда сақтауымыз керек және команда жолына ораламыз, мұнда private subnet-тегі жеке инстансқа ағымдағы қосылымымыз бар және осы жерде ping арқылы сынақ инстансының жеке IP мекенжайына қосылып көреміз.

00:21:13.280 --> 00:21:33.160

Сіз ping өтіп жатқанын, пакеттер алмасатынын көресіз және бұл жеке инстанс public subnet-тегі сынақ инстансымен байланыса алатынын көрсетеді.

00:21:33.160 --> 00:21:43.600

Енді кастомдық Network ACL-ге өзгертулер енгізуіміз керек, бұл Network ACL private subnet-ке байланысты екенін еске саламын.

00:21:43.600 --> 00:21:51.320

Мұнда белгілі бір IP мекенжайы үшін барлық ICMP IPv4 трафигіне тыйым салу керек.

00:21:51.320 --> 00:21:59.640

Бір IP мекенжайын көрсету қажет болғанда, бір IP мекенжайы бар 32 өлшемді CIDR блогы пайдаланылады.

00:21:59.640 --> 00:22:05.400

Бұл ереженің басымдығы оның жұмыс істеуі үшін басқа ережелерден жоғары болуы керек екенін ескеріңіз.

00:22:05.400 --> 00:22:19.960

Ping командасы орындалып жатқан Terminal-ды жаппай, пакеттерді жіберуге рұқсат етейік.

00:22:19.960 --> 00:22:27.800

Network ACL өзгертулерін сақтағаннан кейін, пакеттердің алмасуы тоқтағанын көресіз.

00:22:27.800 --> 00:22:36.800

Бұл Network ACL арқылы кіруді тыйым салынған және қауіпсіздіктің қосымша қабатын қосқанымызды көрсетеді.

00:22:36.800 --> 00:23:00.360

Енді public subnet-тегі сынақ инстансы үшін арнайы кіруге рұқсат бермейтін кастомдық Network ACL бар екенін көресіз.

00:23:00.360 --> 00:23:09.800

Мұның бәрі дұрыс жұмыс істесе, бұл параметрлерді дұрыс енгізгеніңізді білдіреді, осымен тапсырмалардың соңғы блогына жеттік.

00:23:09.800 --> 00:23:26.040

Мұнда зертханалық жұмыстың негізгі парақшасында Details батырмасын басу керек, содан кейін ашылмалы мәзірде Access the multiple choice questions сілтемесін басу керек.

00:23:26.040 --> 00:23:27.800

Ол 6 сұрақтан тұрады.

00:23:27.800 --> 00:23:31.480

Сұрақтардың әрқайсысына тоқталайық.

00:23:31.480 --> 00:23:33.840

Бірінші сұрақ келесідей.

00:23:33.840 --> 00:23:47.760

Public subnet-тегі Internet gateway-дің мақсаты қандай?

00:23:47.760 --> 00:23:48.760

Келесі екінші сұрақ.

00:23:48.760 --> 00:24:01.480

Private subnet-тегі инстансына Интернетке қосылуға және жаңартуларды жүктеп алуға не мүмкіндік береді?

00:24:01.480 --> 00:24:02.480

Үшінші сұрақ.

00:24:02.480 --> 00:24:08.960

Private subnet-тегі инстанс Интернетке тікелей қосыла ала ма?

00:24:08.960 --> 00:24:10.400

Төртінші сұрақ.

00:24:10.400 --> 00:24:21.640

Неліктен біз private subnet-тегі инстансқа және public subnet-тегі инстансқа, атап айтқанда, bastion host үшін екі бөлек кілт жасадық?

00:24:21.640 --> 00:24:22.640

Бесінші сұрақ.

00:24:22.640 --> 00:24:34.520

Bastion host ping командасын сәтті қосып, private subnet-тегі инстанстан жауап ала ала ма?

00:24:34.520 --> 00:24:36.480

Бұл өте жақсы сұрақ.

00:24:36.480 --> 00:24:37.480

Алтыншы сұрақ.

00:24:37.480 --> 00:25:06.400

Private subnet-тегі инстанстың Security тобындағы қандай ереже осы инстанстан public subnet-тегі сынақ инстансына жіберілген ping командасының кіріс трафигіне рұқсат береді?

00:25:06.400 --> 00:25:21.120

Сұрақтар бар парақшада жауап нұсқалары болады, оларды талдап, дұрыс жауап беру үшін дұрыс емес жауап нұсқаларын алып тастау әдісін қолдануға болады.

00:25:21.120 --> 00:25:36.880

AWS Management Console-де орындалатын әрекеттерді бірнеше рет қайталауға болатынын ескеріңіз.

00:25:36.880 --> 00:25:49.680

Тапсырманы жіберу үшін зертханалық жұмыстың негізгі парақшасында Submit батырмасын басып, автобағалау скриптін орындап жатқаныңызды растау керек.

00:25:49.680 --> 00:26:00.040

Зертханалық жұмыс ауқымды болғандықтан, ол сәтті аяқталғанша біраз уақыт күту керек және жинаған ұпайларыңызды парақшаның оң жағында көресіз.

00:26:00.040 --> 00:26:15.760

Егер максималды ұпай жинай алмасаңыз, онда әрқашан қай қадамда, қай тапсырмада ұпайыңыз жеткіліксіз екенін қарап, сол тапсырмаға оралып, оны қайталап орындауыңызға болады.

00:26:15.760 --> 00:26:28.360

Қажетті өзгерістерді енгізгеннен кейін, автоматты бағалау скриптін қайта іске қосып, зертханалық жұмыстың аясында алған ұпайларды жаңартуға болады.

00:26:28.360 --> 00:26:34.400

Зертханалық жұмысты орындағаннан кейін, барлық жүйелерден дұрыс шығуыңыз керек.

00:26:34.400 --> 00:26:40.620

Ең алдымен, AWS Management Console жүйесінен шығуыңыз керек.

00:26:40.620 --> 00:26:53.600

Әрі қарай, зертханалық жұмыстың негізгі парақшасында End lab батырмасын басып, зертханалық жұмысты аяқтағаныңызды растау керек, содан кейін зертханалық жұмыс парақшасын жабу керек.

00:26:53.600 --> 00:26:59.080

Осымен біздің зертханалық жұмысқа шолу сессиямыз аяқталды.

00:26:59.080 --> 00:27:03.200

Бұл өте қызықты зертханалық жұмыс және сізге ұнады деп үміттенемін.

00:27:03.200 --> 00:27:05.760

Сұрақтарыңыз болса, сұраңыз.

00:27:05.760 --> 00:27:11.960

Назарларыңызға рахмет, келесі белсенділіктерде кездескенше.