WEBVTT

00:00:00.000 --> 00:00:07.000

Қайырлы күн, құрметті студенттер! Келесі зертханалық жұмысты талдау сессиясында көргеніме қуаныштымын.

00:00:07.000 --> 00:00:16.000

Бүгінгі зертханалық жұмыстың тақырыбы - кафе бизнес-кейсіміз аясында VPC және оның барлық компоненттерін құру.

00:00:16.000 --> 00:00:18.000

Ендеше, бастайық.

00:00:21.000 --> 00:00:26.000

Зертханалық жұмысты талдауды AWS Management Console негізгі парақшасынан бастаймыз.

00:00:26.000 --> 00:00:35.000

Мұнда VPC сервисіне бару керек. Ол үшін сервисті іздеу жолағын пайдаланып, VPC деп енгіземіз.

00:00:35.000 --> 00:00:38.000

Ең бірінші сілтеме - бізге қажет сілтеме.

00:00:38.000 --> 00:00:48.000

VPC сервисінің негізгі парақшасында сол жақтағы шарлау мәзірін пайдаланып, бар VPC бөліміне өту керек.

00:00:48.000 --> 00:00:59.000

Мұнда зертханалық жұмыстың аясында Lab VPC жасалғанын көреміз, оның негізінде қалған компоненттерді жасаймыз.

00:00:59.000 --> 00:01:08.000

Бірінші қадам subnets жасау болып табылады. Ол үшін сол жақ шарлау мәзірінен Subnets таңдаңыз.

00:01:08.000 --> 00:01:15.000

Мұнда ашылатын парақшаның жоғарғы оң жағындағы Create Subnet батырмасын басу керек.

00:01:15.000 --> 00:01:22.000

Ең басында VPC - Lab VPC таңдау керек.

00:01:22.000 --> 00:01:27.000

Әрі қарай Subnet name енгізу керек, біздің жағдайда Public subnet.

00:01:27.000 --> 00:01:40.000

Сәл төменде Availability zone таңдау керек. Зертханалық жұмыстың аясында бірінші availability zone болуы керек, us-east-1а.

00:01:40.000 --> 00:01:51.000

Біздің subnet-ке арналған CIDR блогы ретінде зертханалық тапсырмадан мәнді көшіріп, тиісті өріске енгізуіміз керек.

00:01:51.000 --> 00:01:57.000

Кейін парақшаның төменгі жағына жылжып, Create Subnet батырмасын басу керек.

00:01:57.000 --> 00:02:09.000

Батырманы басқаннан кейін, барлық subnets тізімі бар парақшаға бағытталамыз және біздің құрылған subnet арқылы фильтрленеді.

00:02:09.000 --> 00:02:15.000

Енді бұл public subnet-ті шын мәнінде public етуіміз керек.

00:02:15.000 --> 00:02:21.000

Ол үшін сол жақ шарлау мәзіріндегі Internet Gateways пунктіне өтіңіз.

00:02:21.000 --> 00:02:29.000

Мұнда жаңа ресурс жасаймыз, ол үшін жоғарғы оң жақтағы Create Internet gateway батырмасын басыңыз.

00:02:29.000 --> 00:02:38.000

Internet gateway жасау кезінде көп кіріс деректерін енгізудің қажеті жоқ, тек осы ресурстың атын енгізіңіз, бұл - Lab IGW.

00:02:38.000 --> 00:02:41.000

Яғни, Internet Gateway деген сөздің қысқасы.

00:02:41.000 --> 00:02:47.000

Кейін парақшаның төменгі жағындағы Create Internet gateway батырмасын басуға болады.

00:02:47.000 --> 00:02:57.000

Оны істегеннен кейін, біз ресурстың негізгі парақшасына, Internet gateway-ге бағытталамыз және күйдің Detached екенін көресіз.

00:02:57.000 --> 00:03:03.000

Сондай-ақ, жасыл түсті хабарландыруда Attach to VPC батырмасын көресіз.

00:03:03.000 --> 00:03:12.000

Бұл осы Internet gateway-ді VPC-лердің біріне байланыстыруымыз керек дегенді білдіреді, біздің жағдайда бұл - Lab VPC.

00:03:12.000 --> 00:03:21.000

Осы батырманы басайық, параметрлер парақшасына бағытталамыз, мұнда VPC таңдау керек, біздің жағдайда Lab VPC.

00:03:21.000 --> 00:03:27.000

Оны таңдап, парақшаның төменгі жағындағы Attach Internet gateway батырмасын басыңыз.

00:03:27.000 --> 00:03:35.000

Оны істегеннен кейін, Internet gateway осы VPC-ге сәтті байланысқаны туралы сәйкес хабарламаны көресіз.

00:03:35.000 --> 00:03:44.000

Сондай-ақ, күй Attached күйіне өзгергенін және VPC ID өрісінде Lab VPC сілтемесі бар екенін көресіз.

00:03:44.000 --> 00:03:55.000

Енді Route Table баптауымыз керек, ол үшін сол жақтағы шарлау мәзірін қолданып, Route tables пунктін таңдаймыз.

00:03:55.000 --> 00:04:12.000

Мұнда, біз білетініміздей, VPC құру кезінде әдепкі Route table жасалады, оны пайдалана аламыз және public subnet-ке қажетті routes-тарды жасай аламыз.

00:04:12.000 --> 00:04:20.000

Біздің жағдайда бірнеше Route tables пайда болуы мүмкін, VPC бағанына қарап дұрыс кестелерді таба аласыз.

00:04:20.000 --> 00:04:41.000

Ол жерде VPC ID және VPC атауы болады. Оны таңдап алайық және осы ресурстың деректері бар парақша ашылатын блокта Routes қойындысын таңдап, Edit routes батырмасын басыңыз.

00:04:41.000 --> 00:04:51.000

Келесі парақшада Destination ретінде бүкіл Интернетті көрсетуіміз керек және біз Интернетке Internet gateway арқылы кіреміз.

00:04:51.000 --> 00:04:57.000

Қажетті өрістерді толтырғаннан кейін өзгертулерді сақтаймыз.

00:04:57.000 --> 00:05:12.000

Мұны орындағаннан кейін сәйкес хабарламаны көреміз, енді subnets парақшасына өтсек, Public subnet-ті көреміз және барлық қажетті компоненттер жасалған.

00:05:12.000 --> 00:05:30.000

Және ол тек атымен ғана емес, шын мәнінде Public subnet болып табылады, осы subnet-те жасалған ресурстар Интернетке кіре алады және Интернеттен осы subnet-тегі ресурстарға қол жеткізуге болады.

00:05:30.000 --> 00:05:37.000

Келесі қадам - ​​Bastion host жасау. Ол үшін EC2 сервисін қолданамыз.

00:05:37.000 --> 00:05:42.000

Ол үшін сервистерді іздеу жолағына EC2 деп теріп, бірінші сілтемеге өту керек.

00:05:42.000 --> 00:05:51.000

EC2 сервисінің негізгі парақшасына өткеннен кейін, Launch instance батырмасын басуымыз керек, кіріс деректерін енгізу парақшасына бағытталамыз.

00:05:51.000 --> 00:06:04.000

Name ретінде Bastion Host, операциялық жүйе ретінде Amazon Linux және AMI ретінде Amazon Linux 2 AMI (HVM) таңдаймыз.

00:06:04.000 --> 00:06:12.000

Біраз төмен айналдырайық, Instance Type ретінде t2.micro таңдау керек болады, егер бұл опция қол жетімді болмаса, t3.micro таңдаңыз.

00:06:12.000 --> 00:06:20.000

Key pair ретінде vockey таңдаңыз және Network settings бөлімінде Edit батырмасын басу керек.

00:06:20.000 --> 00:06:22.000

Біраз өзгерістер енгізетін боламыз.

00:06:22.000 --> 00:06:29.000

VPC ретінде Lab VPC таңдау керек, Subnet ретінде біз жасаған Public subnet таңдаңыз.

00:06:29.000 --> 00:06:40.000

Auto-assign public IP өрісінде оны өшіру керек, өйткені біз Elastic IP address жасап, оны осы инстансқа байланыстырамыз.

00:06:40.000 --> 00:06:47.000

Одан кейін Create security group опциясын таңдап, Bastion Host SG атауын енгізу керек.

00:06:47.000 --> 00:06:59.000

Содан кейін Inbound security group rules бөліміндегі Add security group rule батырмасын басып, келесі rule-ды қосу керек.

00:06:59.000 --> 00:07:13.000

SSH трафигіне рұқсат етеміз, Source ретінде MyIP көрсетеміз, CIDR блок өлшемі 32 болатын жалпы IP мекенжайымды енгіземіз, онда бір IP мекенжайы бар.

00:07:13.000 --> 00:07:21.000

Description ретінде болашақта оның не үшін жасалғанын түсіну үшін кейбір мәндерді көрсету қажет.

00:07:21.000 --> 00:07:25.000

Менің жағдайда, бұл SSH және Yelzhan, яғни пайдаланушы аты.

00:07:25.000 --> 00:07:34.000

Осы параметрлердің барлығын енгізгеннен кейін, парақшаның оң жағындағы Launch instance батырмасын басамыз.

00:07:34.000 --> 00:07:55.000

Инстансты құру басталғаны туралы хабары бар парақшаға бағытталамыз, инстанстың ID бар сілтемені басып, инстанстар тізімі бар және біздің инстансымыз бойынша фильтрленген парақшаға өте аламыз.

00:07:55.000 --> 00:08:11.000

Біраз уақыттан кейін инстанс күйі Running күйіне ауысады және біз келесі ресурстарды жасауды жалғастырамыз, бұл Elastic IP address.

00:08:11.000 --> 00:08:17.000

Ол үшін сол жақ шарлау мәзірінде Elastic IPs опциясын таңдаңыз.

00:08:17.000 --> 00:08:31.000

Мұнда Allocate Elastic IP address батырмасын басу керек және кіріс деректерін енгізу парақшасында Amazon's pool of IPv4 addresses опциясын таңдаңыз.

00:08:31.000 --> 00:08:40.000

Барлық басқа параметрлерді әдепкі ретінде қалдырамыз, парақшаның төменгі жағына жылжып, Allocate батырмасын басыңыз.

00:08:40.000 --> 00:08:59.000

Оны жасағаннан кейін Elastic IP address тізімі бар парақшаға бағытталамыз, хабарда осы Elastic IP address-ті ресурспен байланыстыруыңыз керек екенін көресіз, енді оны жасайық.

00:08:59.000 --> 00:09:09.000

Опциялардың бірі – парақшаның жоғарғы жағындағы Associate this Elastic IP address батырмасын басу немесе осы Elastic IP address-ті таңдау.

00:09:09.000 --> 00:09:18.000

Әрі қарай, Actions батырмасын басып, ашылмалы мәзірден Associate Elastic IP address опциясын таңдаңыз. Сол парақшаға бағытталамыз.

00:09:18.000 --> 00:09:25.000

Параметрлер парақшасында оны қай ресурспен байланыстыратынымызды таңдауыңыз керек: Network interface немесе Instance.

00:09:25.000 --> 00:09:38.000

Біздің жағдайда, бұл - Instance. Оны таңдаған соң, төмендегі өрісте Bastion Host атауы бар EC2 инстансын таңдауымыз керек.

00:09:38.000 --> 00:09:45.000

Оны істегеннен кейін, парақшаның төменгі жағына жылжып, Associate батырмасын басамыз.

00:09:45.000 --> 00:09:57.000

Біз Elastic IP address ресурспен, белгілі бір ID бар инстанспен сәтті байланыстырылғаны туралы хабарлама аламыз.

00:09:57.000 --> 00:10:10.000

Бұл EC2 инстансы Интернетке кіру мүмкіндігінен басқа, Интернеттен де қол жетімді және статикалық IP мекенжайы арқылы қол жеткізуге болатынын білдіреді.

00:10:10.000 --> 00:10:19.000

Бұл IP мекенжайын экранда көресіз.

00:10:19.000 --> 00:10:27.000

Енді public subnet-тегі EC2 инстансына шынымен қосыла алатынымызды тексерейік.

00:10:27.000 --> 00:10:39.000

Ол үшін private key жүктеп алу керек. Зертханалық жұмыстың парақшасына ораламыз, Details батырмасын басыңыз және ашылмалы тізімде Show батырмасын басыңыз.

00:10:39.000 --> 00:10:55.000

Қалқымалы терезеде PPK кілтін жүктеп алу қажет, егер Windows операциялық жүйесі болса, Linux немесе MacOS операциялық жүйесімен жұмыс істеп жатсаңыз, PEM кілтін жүктеп алуыңыз қажет.

00:10:55.000 --> 00:11:03.000

Оны істегеннен кейін, Windows операциялық жүйесі жағдайында PuTTY бағдарламасын жүктеп алу қажет болады.

00:11:03.000 --> 00:11:14.000

Бұл бағдарламамен алдыңғы зертханалық жұмысымызда бірнеше рет жұмыс істедік, сондықтан ол орнатылған, оны іске қосу керек.

00:11:14.000 --> 00:11:24.000

Сондай-ақ, алдында басқа инстанстарға PPK кілтін пайдаланып қосылған болатынбыз.

00:11:24.000 --> 00:11:38.000

Егер сізде сақталған сессия болса, оны жүктей аласыз, содан кейін IP мекенжайы өрісіне Elastic IP ресурсының IP мекенжайын енгізіңіз.

00:11:38.000 --> 00:12:00.000

Ал егер ашылған сессия болмаса, PuTTY бағдарламасының сол жақ шарлау мәзірінде Connection, содан кейін SSH, содан кейін Auth and Credentials жолы бойынша өтіп, сол жерде сәйкес өріс үшін жеке кілттің жолын көрсетуге болады.

00:12:00.000 --> 00:12:10.000

Осыдан кейін бірінші Session қойындысына оралып, EC2 инстансының жалпы IP мекенжайын енгізіңіз.

00:12:10.000 --> 00:12:22.000

Барлық қажетті параметрлерді енгізгеннен кейін Open батырмасын басамыз. Команда жолы ашылады және сіз осы инстансқа бірінші рет қосылсаңыз, осыған ұқсас хабарды көресіз.

00:12:22.000 --> 00:12:42.000

Бұл біз жасаған инстанс болғандықтан, біз оған сенеміз, Accept батырмасын басамыз. Барлық басқа жағдайларда сенімді инстансқа қосылып жатқаныңызға көз жеткізуіңіз керек, содан кейін ғана қосылымды растайсыз.

00:12:42.000 --> 00:13:02.000

Accept батырмасын басқаннан кейін, Amazon Linux үшін әдепкі пайдаланушылар ec2-user көрсетуіміз керек. Enter пернесін басқанда, сәтті авторизацияланғандығымыз туралы хабарламаны және командаларды енгізуге болатын промпт көреміз.

00:13:02.000 --> 00:13:18.000

Бұл public subnet-тегі EC2 инстансына оның жалпы IP мекенжайын пайдаланып қашықтан сәтті қосыла алдық дегенді білдіреді. Жақсы, құттықтаймын, бұл тапсырманы орындап, келесі тапсырмаға көшеміз.

00:13:18.000 --> 00:13:32.000

Келесі тапсырманың аясында private subnet және оған қажетті барлық компоненттерді жасауымыз керек. Ол үшін сервис іздеу жолағына VPC деп енгізуді бастаймыз және сәйкес сервиске барамыз.

00:13:32.000 --> 00:13:48.000

Содан кейін сол жақ шарлау мәзірі арқылы Subnets пунктін таңдаңыз. Бұл жерде жаңа subnet жасау керек, ол үшін Create Subnet батырмасын басыңыз және кіріс деректерін енгізу үшін ашылатын парақшада осы деректерді енгізуді бастаймыз.

00:13:48.000 --> 00:14:04.000

VPC ID ретінде Lab VPC таңдаймыз және Subnet name ретінде Private subnet жазуымыз керек. Сәл төменде Availability zone ретінде осы аймақтағы бірінші availability zone таңдаңыз, біздің жағдайда us-east-1а.

00:14:04.000 --> 00:14:24.000

Ал CIDR блок мәнін зертханалық тапсырма парақшасынан көшіру қажет, ол 10.0.1.0/24. Осы деректерді енгізгеннен кейін парақшаның төменгі жағына жылжып, Create Subnet батырмасын басамыз.

00:14:24.000 --> 00:14:37.000

Subnet сәтті жасалғанын көреміз, енді келесі компоненттерді жасаймыз, ол үшін сол жақ шарлау мәзірін қолданамыз және NAT gateways пунктіне өтеміз.

00:14:37.000 --> 00:14:50.000

Бізде NAT gateway жасалмаған, сондықтан Create NAT gateway батырмасын басайық. Мұнда ашылатын парақшада кіріс деректерінде Name ретінде Lab NAT gateway енгізіңіз.

00:14:50.000 --> 00:15:01.000

Әрі қарай, Subnet ретінде Public subnet таңдаймыз, яғни біздің NAT gateway public subnet-те орналасады және private subnet-тегі ресурстарға Интернетке қосылуға мүмкіндік береді.

00:15:01.000 --> 00:15:12.000

Біраз төмен айналдырайық және NAT gateway жасау кезінде оны жалпыға ортақ статикалық IP мекенжайымен байланыстыру керек екенін есте ұстаймыз.

00:15:12.000 --> 00:15:29.000

Allocate IP address батырмасын басу арқылы Elastic IP ресурсын жасауға болады және оны NAT gateway құру аясында жасап жатқандықтан, Elastic IP ID сәйкес өріске енгізіледі.

00:15:29.000 --> 00:15:36.000

Осыдан кейін парақшаның төменгі жағына жылжып, Create NAT gateway батырмасын басуымыз керек.

00:15:36.000 --> 00:15:46.000

NAT gateway жасағаннан кейін, соңғы қадам қалады, бұл - route table-мен жұмыс.

00:15:46.000 --> 00:15:52.000

Сол жақ шарлау мәзірін пайдаланып, Route tables өтуіңіз керек.

00:15:52.000 --> 00:16:01.000

Алдында public subnet-ке байланыстыру үшін әдепкі route table пайдаландық.

00:16:01.000 --> 00:16:08.000

Енді private subnet-ке байланыстыру үшін бөлек route table жасау керек.

00:16:08.000 --> 00:16:20.000

Сонымен, Create route table батырмасын басайық, кіріс деректерін енгізу үшін ашылатын парақшада Private route table атауын енгізіп, VPC ретінде Lab VPC таңдау керек.

00:16:20.000 --> 00:16:23.000

Осыдан кейін Create route table батырмасын басамыз.

00:16:23.000 --> 00:16:31.000

Біздің route table жасалады және біз ресурстың негізгі парақшасына өтеміз.

00:16:31.000 --> 00:16:40.000

Мұнда Routes қойындысында VPC ішіндегі ресурспен байланысуға көмектесетін бір ғана әдепкі rule бар екенін көреміз.

00:16:40.000 --> 00:16:48.000

Edit routes батырмасын басуымыз керек және мұнда жаңа route қосуымыз керек.

00:16:48.000 --> 00:16:54.000

Destination ретінде Интернеттің белгісін көрсетуіңіз керек, барлығы нөлдер, қиғаш сызық және нөлдер.

00:16:54.000 --> 00:17:04.000

Әрі қарай, Target ретінде NAT gateway көрсетеміз, яғни private subnet-те орналасқан ресурстар Интернетке NAT gateway арқылы қосылады.

00:17:04.000 --> 00:17:06.000

Біздің NAT gateway public subnet-те орналасқан.

00:17:06.000 --> 00:17:13.000

Осы екі өрісті толтырғаннан кейін, Save changes батырмасын басамыз.

00:17:13.000 --> 00:17:18.000

Жақсы, route table дайындап қойдық.

00:17:18.000 --> 00:17:29.000

Route table тәуелсіз бөлек ресурс екенін және кастомдық route table-де жұмыс істеп жатсаңыз, оны subnet-ке нақты байланыстыруыңыз керек екенін ұмытпаңыз.

00:17:29.000 --> 00:17:47.000

Алдында route table-ді subnet-ке байланыстырудың қажеті жоқ еді, себебі ол әдепкі route table болды және әдепкі route table VPC ішінде жасалған барлық subnet-термен байланысады.

00:17:47.000 --> 00:17:57.000

Біздің жағдайда, біз кастомдық route table жасадық және мұнда оны private subnet-ке нақты байланыстыру керек.

00:17:57.000 --> 00:18:06.000

Ол үшін Subnet associations қойындысына өтіп, Edit subnet associations батырмасын басыңыз.

00:18:06.000 --> 00:18:15.000

Біз subnet бар парақшаға бағытталамыз, VPC ішіндегі қолжетімді барлық subnet-тер осы жерде көрсетіледі.

00:18:15.000 --> 00:18:18.000

Сіз public subnet және private subnet бар екенін көресіз.

00:18:18.000 --> 00:18:28.000

Олардың екеуі де әдепкі route table-ге байланысты, оны сәйкес бағанда көруге болады, осы кестедегі соңғы баған.

00:18:28.000 --> 00:18:37.000

Бұл парақшада private subnet таңдап, Save associations батырмасын басу керек.

00:18:37.000 --> 00:18:38.000

Нәтижесінде не болады?

00:18:38.000 --> 00:18:50.000

Subnet-ті бір уақытта тек бір route table-мен байланыстыруға болатынын, ал бір route table-ді бірнеше subnet-терде пайдалануға болатынын есте ұстаймыз.

00:18:50.000 --> 00:19:07.000

Сондықтан private subnet-тің әдепкі route table-мен байланысы жойылады және кастомдық route table мен private subnet-тің жаңа байланысы жасалады.

00:19:07.000 --> 00:19:14.000

Жақсы, оны жасағаннан кейін Subnet associations тізімінде private subnet көре аламыз.

00:19:14.000 --> 00:19:28.000

Сондай-ақ, осындай ID бар route table біздің private subnet-ке сәтті қосылғаны туралы хабарламаны көреміз.

00:19:28.000 --> 00:19:42.000

Барлық қажетті параметрлерді жасадық, енді бәрі дұрыс жұмыс істеп тұрғанын және Интернеттен private subnet-те орналасқан ресурстарға қосылу мүмкіндігін тексеру керек.

00:19:42.000 --> 00:19:56.000

Ол үшін инстанс жасау керек, EC2 сервисіне өтіңіз, содан кейін EC2 сервисінің негізгі парақшасында Launch instance батырмасын басып, кіріс деректерін енгізуді бастау керек.

00:19:56.000 --> 00:20:07.000

Name ретінде Private instance көрсетеміз, операциялық жүйе ретінде Amazon Linux таңдаймыз, ал AMI ретінде Amazon Linux 2 AMI (HVM) таңдаймыз.

00:20:07.000 --> 00:20:17.000

Instance type ретінде t2.micro таңдаймыз және жеке кілт бөлімінде жаңасын жасау керек болады.

00:20:17.000 --> 00:20:32.000

Ол үшін Create new key pair батырмасын басыңыз, алдыңғы жеке кілттен басқа атауды көрсетіңіз, vockey2 болсын және дұрыс форматын таңдау керек.

00:20:32.000 --> 00:20:41.000

Естеріңізге сала кетейін, егер Windows операциялық жүйесімен жұмыс жасасаңыз, PPK форматын таңдауыңыз керек, ол PuTTY бағдарламасына жарамды.

00:20:41.000 --> 00:20:49.000

Ал егер MacOS немесе Linux операциялық жүйесімен жұмыс істеп жатсаңыз, PEM форматын таңдауыңыз керек.

00:20:49.000 --> 00:20:55.000

Жақсы, форматты таңдадық, атын жаздық, енді Create key pair батырмасын басу керек.

00:20:55.000 --> 00:21:03.000

Оны басқаннан кейін, жеке кілтті жергілікті компьютерде сақтау сұралады.

00:21:03.000 --> 00:21:09.000

Бұл жеке кілтті жүктеп алуға болатын жалғыз жағдай, сондықтан оны сақтаймыз.

00:21:09.000 --> 00:21:24.000

Әрі қарай, желі параметрлерінің келесі бөлімінде Lab VPC таңдау керек, Subnet ретінде Private subnet таңдаймыз және сәл төменде Create security group опциясын таңдауымыз керек.

00:21:24.000 --> 00:21:33.000

Жаңа security group құрып жатырмыз, Inbound security group rules бөлімінде жаңа rule қосу керек.

00:21:33.000 --> 00:21:43.000

Мұнда SSH трафигін көрсетеміз, Source type ретінде Custom деп көрсетеміз, ал Source ішінде біздің bastion host-тың security тобын көрсетеміз.

00:21:43.000 --> 00:21:57.000

Бұл тек осы security group байланыстырылған subnet-терді SSH қосылымының бастамашысы ретінде пайдалануға болатындығын білдіреді.

00:21:57.000 --> 00:22:03.000

Бұл инстансқа public subnet-тегі ресурстар ғана қосыла алады.

00:22:03.000 --> 00:22:11.000

Description ретінде бұл rule не үшін жасалғанын түсінуді жеңілдету үшін Bastion host SG көрсетейік.

00:22:11.000 --> 00:22:19.000

Жақсы, барлық қажетті параметрлерді енгіздік, енді экранның оң жағындағы Launch instance батырмасын басуға болады.

00:22:19.000 --> 00:22:27.000

Біздің инстансымыз жасалып жатқанда, келесі сұраққа жауап берейік.

00:22:27.000 --> 00:22:35.000

Бізде public subnet-те жасалған bastion host бар, оған қосыла аламыз, оны тексердік.

00:22:35.000 --> 00:22:42.000

Енді private subnet-те басқа инстанс жасаймыз және оған қосыламыз.

00:22:42.000 --> 00:22:48.000

Біз private subnet-тегі ресурстарға қосылу үшін арнайы bastion host жасадық, бұл жақсы.

00:22:48.000 --> 00:22:58.000

Бірақ оның қалай әрекет ететінін елестетіп көріңізші, bastion host-қа қосылу үшін компьютерде жергілікті түрде сақталған жеке кілтті қолданамыз.

00:22:58.000 --> 00:23:02.000

Және жергілікті компьютерден SSH қосылымын бастаймыз.

00:23:02.000 --> 00:23:28.000

Енді bastion host-тан private subnet-тегі инстансқа SSH қосылымын бастау үшін bastion host-та, яғни жергілікті түрде SSH қосылымын іске қосатын жерде, жеке кілт болуы керек, атап айтқанда біз жасаған кілт және содан кейін жеке инстансқа қосыла аламыз.

00:23:28.000 --> 00:23:40.000

Бұл қауіпсіздік тұрғысынан ең жақсы нұсқа емес, өйткені bastion host барлық қызметкерлер оған қосылатын орын болып табылады, содан кейін сол жақтан қажетті ресурстарға қосылады.

00:23:40.000 --> 00:23:50.000

Компанияда әртүрлі командалар жұмыс істейтіндіктен, олар нәтижесінде қосылатын target-тер әртүрлі болуы мүмкін.

00:23:50.000 --> 00:24:02.000

Және олар әртүрлі жеке кілттерді пайдаланады. Жеке кілтіңізді bastion host-ында сақтасаңыз, басқа пайдаланушылар бұл кілтті пайдаланып, оны рұқсатсыз пайдалана алады.

00:24:02.000 --> 00:24:18.000

Сондықтан, PuTTY бағдарламасының әзірлеу тобы шешім ретінде тағы бір қосымша бағдарлама жасады, ол Pageant деп аталатын PuTTY бағдарламасына арналған плагин ретінде жұмыс істейді.

00:24:18.000 --> 00:24:33.000

Идея мынада: SSH қосылымы іске қосылған жерде барлық кілттерді жергілікті түрде сақтау арқылы инстанстарға дәйекті түрде қосылуға болады.

00:24:33.000 --> 00:24:44.000

Яғни, жергілікті компьютерден жеке кілттерді тек осы компьютерде сақтай отырып, bastion host арқылы private subnet-тегі инстансқа қосыла аламыз.

00:24:44.000 --> 00:24:54.000

Осылайша, бұл бағдарламаны пайдалана отырып, bastion host-ында жеке инстанстың жеке кілтін сақтаудың қажеті жоқ.

00:24:54.000 --> 00:25:03.000

Бұл - өте ыңғайлы және жақсы бағдарлама екен. Енді оның қалай жұмыс істейтінін және оны қалай баптау керектігін көрейік.

00:25:03.000 --> 00:25:14.000

Ең алдымен, оны жүктеп алу керек, орнатудың қажеті жоқ, exe файлын іске қосқан кезде бағдарламаның өзі қосылады және осы жерде Add key батырмасын басу керек.

00:25:14.000 --> 00:25:23.000

Одан кейін кілттеріміздің екеуін де таңдап, олардың жеке кілттер тізімінде пайда болуын қамтамасыз ету керек.

00:25:23.000 --> 00:25:29.000

Осымен Pageant бағдарламасында барлық қажетті параметрлерді жасадық, Close батырмасын басуға болады.

00:25:29.000 --> 00:25:34.000

Әрі қарай, PuTTY бағдарламасында сәйкес функцияны белсендіру керек.

00:25:34.000 --> 00:25:49.000

Сол жақ шарлау мәзірінде Auth парақшасын таңдау керек және парақшаның өзінде Allow agent forwarding опциясына құсбелгі қою керек.

00:25:49.000 --> 00:26:00.000

Бұл әрекетті орындағаннан кейін, bastion host-ының жеке кілтін таңдауыңыз керек, бұл Credentials парақшасында.

00:26:00.000 --> 00:26:07.000

Ең бірінші өрісте Browse батырмасын басып, PPK кілтінің жолын көрсету керек.

00:26:07.000 --> 00:26:16.000

Осыдан кейін bastion host-ының жалпыға ортақ IP мекенжайын көшіру керек болады, оны екі жолмен жасай аламыз.

00:26:16.000 --> 00:26:25.000

Біріншісі - EC2 инстанстарының тізімінде, егер bastion host таңдасаңыз, метадеректерде сәйкес өріс бар.

00:26:25.000 --> 00:26:32.000

Сондай-ақ, Elastic IP мекенжайларының тізімінде жалпыға ортақ IP мекенжайын қарай аламыз.

00:26:32.000 --> 00:26:41.000

IP мекенжайын көшіргеннен кейін, оны PuTTY бағдарламасына қойып, Open батырмасын басуымыз керек.

00:26:41.000 --> 00:26:56.000

Мұнда пайдаланушы атын енгізу керек, ec2-user, Enter пернесін басыңыз, сонда командаларды енгізуге болатын промпт көресіз, бұл bastion host-ымызға сәтті қосылғанымызды білдіреді.

00:26:56.000 --> 00:27:00.000

Жеке IP мекенжайы осы жерде көрсетіледі.

00:27:00.000 --> 00:27:06.000

Енді private subnet-тегі инстансқа қосылып көруіміз керек.

00:27:06.000 --> 00:27:14.000

Ол үшін EC2 инстанстарының тізімі бар парақшаға ораламыз және private instance таңдаймыз.

00:27:14.000 --> 00:27:25.000

Оның жалпыға ортақ IP мекенжайы жоқ екенін ескеріңіз, бұл дұрыс, себебі бұл инстанс private subnet-те жасалған және оған Интернеттен қосыла алмайсыз.

00:27:25.000 --> 00:27:42.000

Бірақ оның жеке IP мекенжайы бар және оны пайдаланатын боламыз, өйткені bastion host пен бұл private instance бір VPC-де орналасқандықтан, олар бір-бірімен жеке IP мекенжайлары арқылы қосыла алады.

00:27:42.000 --> 00:28:04.000

Осы мәнді көшіріп алып, келесі команданы қосамыз, SSH, пайдаланушы аты ec2-user және ит белгісі арқылы private subnet-тегі инстанстың жеке IP мекенжайын жазамыз.

00:28:04.000 --> 00:28:15.000

Команданы жазғаннан кейін, Enter пернесін басыңыз, содан кейін осы инстансқа шынымен қосылғымыз келетінін растаңыз, Yes деп, Enter пернесін басыңыз.

00:28:15.000 --> 00:28:23.000

Осыдан кейін промпт пайда болғанын және IP мекенжайының өзгергенін көресіз, бұл біздің private instance-тың IP мекенжайы.

00:28:23.000 --> 00:28:33.000

Жақсы, құттықтаймын, private subnet-тегі private instance-қа сәтті қосыла алдық.

00:28:33.000 --> 00:28:46.000

Енді соңғы тексеру үшін private subnet-тегі бұл инстанстың Интернетке шынымен қол жеткізе алатынына көз жеткізуіміз керек.

00:28:46.000 --> 00:29:01.000

Ол үшін келесі ping командасын және барлық сегіздігі бар IP мекенжайы DNS google немесе сізге таныс кез келген веб-сайттың URL мекенжайын енгізіңіз.

00:29:01.000 --> 00:29:19.000

Енді ping командасын енгізіп, google.com сайтына кірейік, бірінші және екінші жағдайда пакеттер сәтті алмасуын көресіз, бұл private subnet-тегі инстанстардың Интернетке қол жетімді екенін көрсетеді.

00:29:19.000 --> 00:29:30.000

Егер солай болса, бұл осы уақытқа дейін барлық қажетті параметрлерді дұрыс жасағанымызды, бәрі дұрыс бапталғанын білдіреді.

00:29:30.000 --> 00:29:41.000

Келесі тапсырмаға көшеміз және бізде тағы бір компонент қалды, бұл Network ACL, VPC компоненті, ол қосымша қорғаныс қабаты болып табылады.

00:29:41.000 --> 00:29:45.000

Оны қалай жасау керектігін және онымен қалай жұмыс істеуге болатынын көрейік.

00:29:45.000 --> 00:30:04.000

Ол үшін AWS Management Console-де VPC сервисіне барайық. Содан кейін сол жақтағы шарлау мәзірін қолданып, Network ACL опциясын таңдаймыз. Security тобында екі пункт бар екенін ескеріңіз, Network ACL және Security groups.

00:30:04.000 --> 00:30:29.000

Network ACLs тізіміне кіргеннен кейін, Lab VPC-ге байланған әдепкі Network ACL бар екенін ескеріңіз, егер оны таңдап, Metadata бөлімінде Subnet associations қойындысына өтсеңіз, біздің екі subnet-ті көресіз, бұл private және public subnet.

00:30:29.000 --> 00:30:35.000

Олар әдепкі бойынша Default Network ACL-мен байланысты.

00:30:35.000 --> 00:30:41.000

Inbound rules қарасақ, барлық трафикке 100 басымдылықпен рұқсат етілгенін көреміз.

00:30:41.000 --> 00:30:48.000

Бұл inbound rules-тағы ең жоғары басымдық болғандықтан, барлық трафикке рұқсат етіледі.

00:30:48.000 --> 00:30:51.000

Сондай-ақ, бұл Default Network ACL екенін ескеріңіз.

00:30:51.000 --> 00:30:57.000

Default Network ACL үшін барлық кіріс және шығыс трафикке автоматты түрде рұқсат етіледі.

00:30:57.000 --> 00:31:07.000

Оны Outbound rules қойындысында тексере аламыз, 100 басымдылықпен барлық шығыс трафикке рұқсат етілгенін көресіз.

00:31:07.000 --> 00:31:10.000

Енді кастомдық Network ACL жасайық.

00:31:10.000 --> 00:31:15.000

Ол үшін жоғарғы оң жақтағы Create Network ACL батырмасын басу керек.

00:31:15.000 --> 00:31:24.000

Мұнда осы ресурстың атын енгізу керек, Lab Network ACL және VPC ретінде Lab VPC таңдау керек.

00:31:24.000 --> 00:31:29.000

Содан кейін парақшаның төменгі жағындағы Create Network ACL батырмасын басуға болады.

00:31:29.000 --> 00:31:45.000

Біздің кастомдық Network ACL жасалғаннан кейін, осы ресурстардың тізіміне бағытталамыз және сәйкес бағанда Lab Network ACL әдепкі емес Network ACL екенін көресіз.

00:31:45.000 --> 00:31:46.000

Жақсы.

00:31:46.000 --> 00:31:52.000

Енді оны таңдап, Inbound rules бөлімінде қандай rules бар екенін көреміз.

00:31:52.000 --> 00:32:01.000

Сіз inbound және outbound rules үшін трафик әдепкі бойынша тыйым салынғанын көресіз.

00:32:01.000 --> 00:32:06.000

Бұл - кастомдық Network ACL-дің әдепкі әрекеті.

00:32:06.000 --> 00:32:12.000

Енді трафикке рұқсат беру үшін кейбір rules қосайық.

00:32:12.000 --> 00:32:17.000

Ол үшін Edit outbound rules батырмасын басу керек.

00:32:17.000 --> 00:32:30.000

Мұнда Add new rule батырмасын басып, 100 басымдылығымен public subnet-тің CIDR блогына дейінгі барлық трафикке рұқсат беру керек.

00:32:30.000 --> 00:32:33.000

Содан кейін өзгертулерді сақтаймыз.

00:32:33.000 --> 00:32:38.000

Inbound rules үшін де тура сол өзгертулер жасалуы керек.

00:32:38.000 --> 00:32:52.000

100 басымдылығы бар жаңа rule қосамыз, бұл source-қа дейінгі барлық трафикке рұқсат береді, бұл public subnet-тің CIDR блогы және осы өзгерістерді сақтаңыз.

00:32:52.000 --> 00:32:57.000

Network ACL тәуелсіз ресурс екенін еске саламын.

00:32:57.000 --> 00:33:05.000

Сондықтан, кастомдық Network ACL жасағанда, оны қажетті subnet-терге анық байланыстыру керек.

00:33:05.000 --> 00:33:13.000

Біздің жағдайда оны private subnet-ке байланыстырамыз.

00:33:13.000 --> 00:33:17.000

Оны жасағаннан кейін, бір эксперимент жасайық.

00:33:17.000 --> 00:33:23.000

Ол үшін public subnet-те сынақ инстансын жасау керек.

00:33:23.000 --> 00:33:26.000

Ендеше EC2 сервисіне көшейік.

00:33:26.000 --> 00:33:31.000

Launch instance батырмасын басып, кіріс деректерін енгізіңіз.

00:33:31.000 --> 00:33:33.000

Name ретінде Test Instance көрсетеміз.

00:33:33.000 --> 00:33:41.000

Операциялық жүйе ретінде Amazon Linux және AMI ретінде Amazon Linux 2 AMI (HVM) таңдаймыз.

00:33:41.000 --> 00:33:45.000

Instance type ретінде t2.micro таңдайық.

00:33:45.000 --> 00:33:49.000

Жеке кілтті көрсетудің қажеті жоқ, өйткені оған қосылмаймыз.

00:33:49.000 --> 00:33:53.000

Желі параметрлеріне кейбір өзгерістер енгізу қажет болады.

00:33:53.000 --> 00:33:58.000

VPC өрісінде Lab VPC таңдау керек.

00:33:58.000 --> 00:34:04.000

Subnet ретінде Public subnet таңдап, жаңа Security group жасау керек.

00:34:04.000 --> 00:34:12.000

Мұнда Add security group rule батырмасын басып, сәйкес мәндерді енгізу керек.

00:34:12.000 --> 00:34:22.000

IPv4 протоколы арқылы барлық ICMP трафигіне рұқсат етеміз.

00:34:22.000 --> 00:34:30.000

Source type ретінде Anywhere, яғни бүкіл Интернетті көрсетеміз, ал Description ретінде Allow ICMP деп жазамыз.

00:34:30.000 --> 00:34:35.000

Бұл сонымен қатар ping командасы арқылы трафикке мүмкіндік береді.

00:34:35.000 --> 00:34:49.000

Осы өрістердің барлығын толтырғаннан кейін, экранның оң жағындағы парақшаның төменгі жағына жылжып, Launch instance батырмасын басуымыз керек.

00:34:49.000 --> 00:35:00.000

Инстансымыз жасалып жатқанда, Test Instance таңдап, оның жеке IP мекенжайын көшіру керек болады.

00:35:00.000 --> 00:35:14.000

Көшіріп алғаннан кейін, SSH сессиясына ораламыз, онда private subnet-тегі инстансқа қосылып, ping командасын және сынақ инстансымыздың IP мекенжайын іске қосамыз.

00:35:14.000 --> 00:35:17.000

Бұл сынақ инстансы public subnet-те орналасқан.

00:35:17.000 --> 00:35:26.000

Сіз пакеттердің алмасуын, олар сәтті шығып, қайтарылатынын және уақыт көрсетілгенін көресіз.

00:35:26.000 --> 00:35:34.000

AWS Management Console-іне оралайық.

00:35:34.000 --> 00:35:45.000

Мұнда кастомдық Network ACL таңдау керек, содан кейін Outbound rules қойындысында Edit outbound rules батырмасын басыңыз.

00:35:45.000 --> 00:36:15.000

Мұнда енді жоғарырақ басымдылығы бар жаңа rule енгіземіз, ол 50 басымдылық болсын, Type traffic үшін IPv4 бойынша ICMP, Destination үшін бұл сынақ инстансының жеке IP мекенжайы, CIDR блок өлшемі 32, өйткені біз арнайы IP мекенжайын көрсетеміз және Allow/Deny өрісінде Deny көрсетіңіз.

00:36:15.000 --> 00:36:23.000

Яғни, сынақ инстансына ICMP трафигіне тыйым саламыз және осы өзгерістерді сақтаймыз.

00:36:23.000 --> 00:36:33.000

Өзгерістерді сақтағаннан кейін, PuTTY сеансында пакеттердің алмасуы тоқтатылғанын байқайсыз.

00:36:33.000 --> 00:36:45.000

Бағдарламадан шығып, ping командасын және сынақ инстансының жеке IP мекенжайын қайтадан іске қоссақ, пакеттердің алмаспайтынын көресіз.

00:36:45.000 --> 00:36:57.000

Бұл Network ACL қорғанысының қосымша қабатын пайдаланғанымызды және бізді қызықтыратын трафикті CIDR блогына дейін тыйым салғанымызды көрсетеді.

00:36:57.000 --> 00:37:06.000

Біздің жағдайда бұл public subnet-тегі сынақ инстансының IP мекенжайы.

00:37:06.000 --> 00:37:12.000

Жақсы, біз зертханалық жұмыстың барлық тапсырмаларын орындадық, құттықтаймын.

00:37:12.000 --> 00:37:15.000

Тек тест сұрақтарына жауап беру ғана қалды.

00:37:15.000 --> 00:37:22.000

Оларға жету үшін зертханалық жұмыс парақшасындағы Details батырмасын басу керек.

00:37:22.000 --> 00:37:27.000

Содан кейін ашылмалы тізімде Show батырмасын басыңыз.

00:37:27.000 --> 00:37:36.000

Қалқымалы терезеде төменге қарай жылжып, Access the multiple choice questions сілтемесін басу керек.

00:37:36.000 --> 00:37:40.000

Веб-браузерде сұрақтар тізімі бар бөлек парақшаға бағытталасыз.

00:37:40.000 --> 00:37:43.000

Барлығы 6 сұрақ бар.

00:37:43.000 --> 00:37:46.000

Олардың әрқайсысына жауап берейік.

00:37:46.000 --> 00:37:54.000

Ең бірінші сұрақ: Internet gateway мен public subnet не үшін пайдаланылады?

00:37:54.000 --> 00:38:07.000

Бұл видеоны тоқтатып, өзіңіз жауап беріп көріңіз.

00:38:07.000 --> 00:38:20.000

Internet gateway public subnet-тегі ресурстарға және жалпы IP мекенжайы бар ресурстарға Интернетке кіруді қамтамасыз ету үшін пайдаланылады.

00:38:20.000 --> 00:38:23.000

Екінші сұрақ.

00:38:23.000 --> 00:38:31.000

Private subnet-тегі ресурстарға Интернетке кіруге және бағдарламалық құрал жаңартуларын орнатуға не мүмкіндік береді?

00:38:31.000 --> 00:38:39.000

Бұл видеоны тоқтатып, оған өзіңіз жауап беріп көріңіз.

00:38:39.000 --> 00:38:41.000

Дұрыс жауап - NAT gateway.

00:38:41.000 --> 00:38:43.000

Келесі сұраққа көшейік.

00:38:43.000 --> 00:38:47.000

Үшінші сұрақ.

00:38:47.000 --> 00:38:55.000

Private subnet-тегі инстансқа Интернеттен тікелей қол жеткізу мүмкін бе?

00:38:55.000 --> 00:39:03.000

Видеоны тоқтатып, өзіңіз жауап беріп көріңіз.

00:39:03.000 --> 00:39:05.000

Дұрыс жауап – No.

00:39:05.000 --> 00:39:11.000

Яғни, private subnet-тегі инстансқа Интернеттен тікелей қосылу мүмкін емес.

00:39:11.000 --> 00:39:26.000

Осылайша, private subnet-те ресурстарды, атап айтқанда, дерекқорды, мүмкін сіздің қолданбаңыздың логикасы орындалатын инстанстарды сақтай аламыз.

00:39:26.000 --> 00:39:28.000

Төртінші сұрақ.

00:39:28.000 --> 00:39:37.000

Неліктен біз private instance пен bastion host үшін екі түрлі жеке кілтті пайдаландық?

00:39:37.000 --> 00:39:44.000

Видеоны тоқтатып, өзіңіз жауап беріп көріңіз.

00:39:44.000 --> 00:39:55.000

Дұрыс жауап - жеке кілттер істен шыққан жағдайда оның ықтимал зақымдануын азайту үшін біз бөлек кілттерді жасадық.

00:39:55.000 --> 00:40:09.000

Яғни, егер жеке инстанстың жеке кілті жалпыға қолжетімді болса, пайдаланушылар сонда да оған қол жеткізе алмайды, өйткені олар осы кілтпен bastion host-қа қосыла алмайды.

00:40:09.000 --> 00:40:34.000

Әйтпесе, егер bastion host-ының жеке кілті жалпыға қолжетімді болса, онда тек осы bastion host-қа қосылуға болады, содан кейін басқа инстанстарға, сонымен қатар біздің жеке инстансымызға да қосылу мүмкін болмайды, өйткені ол басқа жеке кілт арқылы қосылған.

00:40:34.000 --> 00:40:39.000

Келесі сұрақ.

00:40:39.000 --> 00:40:49.000

Bastion host жағында жеке инстансқа қарай ping командасын іске қосу мүмкін бе және біз жауап ала аламыз ба?

00:40:49.000 --> 00:40:53.000

Мұқият ойланып, өзіңіз жауап беруге тырысыңыз.

00:40:53.000 --> 00:41:05.000

Сұраққа жауап берумен қатар, белгілі бір жауаптың неліктен дұрыс не дұрыс емес екендігі туралы да ойланыңыз.

00:41:05.000 --> 00:41:09.000

Жақсы, дұрыс жауап - No.

00:41:09.000 --> 00:41:11.000

Неге екенін талдайық.

00:41:11.000 --> 00:41:25.000

Жеке инстансқа security group теңшеген кезде, тек SSH трафигі үшін inbound rule жасадық.

00:41:25.000 --> 00:41:40.000

Ping SSH трафигіне жатпайтындықтан, ол басқа трафик түріне жатады, онда bastion host-тан private subnet-тегі инстансқа дейін біз ping командасын сәтті орындай алмаймыз.

00:41:40.000 --> 00:41:48.000

Алтыншы сұрақ та өте жақсы сұрақ.

00:41:48.000 --> 00:42:04.000

Қандай security group rules жеке EC2 инстансына кері трафикті, сынақ инстансына ping жасаудың кері нәтижесін алуға мүмкіндік береді?

00:42:04.000 --> 00:42:11.000

Жеке инстанстың private subnet-те, ал сынақ инстансы public subnet-те екенін еске саламын.

00:42:11.000 --> 00:42:16.000

Видеоны тоқтатып, өзіңіз жауап беріп көріңіз.

00:42:20.000 --> 00:42:33.000

Алтыншы сұраққа дұрыс жауап - private instance-қа арналған outbound rules және сынақ инстансына арналған inbound rules болып табылады.

00:42:33.000 --> 00:42:46.000

Неліктен? Security group - stateful болғандықтан, outbound трафикке рұқсат етілгеніне немесе рұқсат етілмегеніне қарамастан, кірген трафик кері қайтарылады.

00:42:46.000 --> 00:43:00.000

Ал керісінше жағдайда, outbound ретінде рұқсат етілген трафик белгілі бір security group үшін рұқсат етілгеніне немесе рұқсат етілмегеніне қарамастан, ол бәрібір қайтады.

00:43:00.000 --> 00:43:16.000

Сондықтан, ping командасын бастау үшін бізге жеке инстанстың security тобы inbound трафик міндетті түрде қайтарылатынын біле отырып, тиісті outbound rules қамтуы керек.

00:43:16.000 --> 00:43:25.000

Ал сынақ инстансы үшін бұл команда inbound трафик болып табылады, сондықтан inbound трафикке рұқсат беру қажет.

00:43:25.000 --> 00:43:36.000

Security group - stateful болғандықтан, кірген трафик қай outbound ережелері тіркелгеніне қарамастан қайтарылады.

00:43:36.000 --> 00:43:47.000

Осымен біз барлық сұрақтарға жауап алдық. Енді зертханалық жұмысымыздың бағалау нәтижесін қарайық.

00:43:47.000 --> 00:43:55.000

Ол үшін зертханалық жұмыс парақшасында Submit батырмасын басып, оны растап, біраз күту керек.

00:43:55.000 --> 00:44:01.000

Бұл зертханалық жұмыс айтарлықтай ауқымды болғандықтан, тексеру біраз уақытты алады.

00:44:01.000 --> 00:44:15.000

Бағалау скрипті іске қосылғаннан кейін ұпайларыңызды көресіз. Менің жағдайымда 56 ұпайдан 56 ұпай жинадым, бұл барлық тапсырмаларды дұрыс орындадық, сонымен қатар барлық сұрақтарға дұрыс жауап бердік дегенді білдіреді.

00:44:15.000 --> 00:44:29.000

Егер максималды балл болмаса, онда аздап төмен жылжып, қай жерде жетіспейтін ұпайларды көре аласыз, оны түзетіп, бағалауды қайта өткізе аласыз.

00:44:29.000 --> 00:44:39.000

Егер максималды ұпай жинасаңыз, құттықтаймын. Жақсы. Енді барлық жүйелерден дұрыс шығуымыз керек.

00:44:39.000 --> 00:44:51.000

Бұл, ең алдымен, AWS Management Console-ге қатысты. Жоғарғы оң жақтағы пайдаланушы атын басып, ашылмалы тізімдегі Sign out батырмасын басу керек.

00:44:51.000 --> 00:44:57.000

Әрі қарай, зертханалық жұмыс парақшасына оралып, End lab батырмасын басыңыз.

00:44:57.000 --> 00:45:06.000

Зертханалық жұмысты аяқтағанымызды растаңыз және зертханалық жұмыстың парақшасын жабуға болатындығы туралы хабарды күтіңіз.

00:45:06.000 --> 00:45:16.000

Осымен зертханалық жұмысты талдау сессиясы аяқталды. Бұл өте ауқымды зертханалық жұмыс болды.

00:45:16.000 --> 00:45:26.000

VPC барлық құрамдас бөліктерімен таныстық және VPC және оның құрамдас бөліктері туралы толық түсінікке ие болдыңыз деп үміттенемін.

00:45:26.000 --> 00:45:32.000

Назар аударғаныңызға рахмет. Келесі белсенділіктерде кездескенше.