WEBVTT

00:00:00.000 --> 00:00:04.600

Қайырлы күн, құрметті студенттер! Барлықтарыңызды келесі дәрісте көргеніме қуаныштымын.

00:00:04.600 --> 00:00:07.400

Бүгінгі дәрісіміздің тақырыбы - Connecting networks.

00:00:07.400 --> 00:00:14.920

Алдында VPC неден тұратыны және оның қандай компоненттері бар екендігі туралы айтқан болатынбыз.

00:00:14.920 --> 00:00:31.000

Енді бір деңгейге көтеріліп, AWS бұлтындағы желілерді, сондай-ақ AWS бұлтындағы желіні бұлттан тыс жергілікті желімен қалай қосуға болатынын қарастырамыз.

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

Ендеше, бастайық.

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

Бүгінгі дәрісімізде 6 тақырыпты қарастырамыз.

00:00:38.000 --> 00:00:43.200

Бірінші тақырып зертханалық жұмысымызға қатысты және қандай компоненттер қосылатынын көрейік.

00:00:43.200 --> 00:00:51.000

Келесі, екінші және үшінші бөлімдерде жергілікті инфрақұрылымды AWS бұлтына қалай қосу керектігін қарастырамыз.

00:00:51.000 --> 00:01:01.600

Әрі қарай, төртінші және бесінші бөлімдерде VPC-лерді AWS бұлтында бір-біріне қалай қосуға болатынын қарастырамыз.

00:01:01.600 --> 00:01:07.400

Ең соңында, VPC-мен біріктірілген қосымша сервистерді қарастырамыз.

00:01:07.400 --> 00:01:17.200

Дәрісіміздің бірінші бөлімін бастаймыз және зертханалық жұмыстың аясында қандай міндеттер тұрғанын қарастырамыз.

00:01:17.200 --> 00:01:29.200

Бизнес-кейсімізге сәйкес, кафе жаппай сатылым жариялады. Егер сатып алушы 10 немесе одан да көп бірдей зат сатып алса, онда сыйлық ретінде бір десерт беріледі.

00:01:29.200 --> 00:01:36.000

Бірақ сатып алушылардың процесін бақылау үшін кейбір жеке ақпаратты сақтау керек.

00:01:36.000 --> 00:01:39.400

Бұл - электрондық пошта мекенжайы мен несие картаның нөмірі.

00:01:39.400 --> 00:01:54.400

София және басқа басты кейіпкерлер орналасқан нақты елде деректерді сақтауға қатысты кейбір шектеулерге байланысты кафе бұл ақпаратты AWS бұлтында сақтай алмайды.

00:01:54.400 --> 00:02:10.400

Сондықтан, пайдаланушы деректерін сақтайтын жергілікті дерекқорды құру туралы шешім қабылданды, бірақ транзакциялық деректер мен бүкіл инфрақұрылым AWS бұлтында қалады.

00:02:10.400 --> 00:02:23.400

Бұл деректер қажет болған кезде AWS бұлтынан жергілікті инфрақұрылымға, атап айтқанда бізге қажет дерекқорға тікелей сұраныс келіп, қажетті деректерді шығарады.

00:02:23.400 --> 00:02:28.400

Тағы VPC-ге қатысты бір мәселені айта кетейін.

00:02:28.400 --> 00:02:36.400

Бізде Dev ортасы, сондай-ақ Prod ортасы бар екенін есте ұстаймыз. Екеуі де бір VPC-де орналасқан.

00:02:36.400 --> 00:02:49.400

София Оливиямен кеңескеннен кейін, оларды ажырату керек деп шешеді. Яғни, Dev ортасы бөлек оқшауланған VPC-де, ал Prod ортасы басқа VPC-де.

00:02:49.400 --> 00:03:02.400

Бірақ, соған қарамастан, Оливия Софияға оларды бір-бірімен қосымша байланыстыруға кеңес береді, осылайша Dev ортасынан Prod ортасындағы ресурстарға қол жеткізе алатын болады.

00:03:02.400 --> 00:03:19.400

Көріп отырғаныңыздай, зертханамыздың аясында AWS бұлтындағы бірнеше VPC-мен жұмыс істейміз, сонымен қатар AWS бұлтындағы және жергілікті инфрақұрылымдағы VPC-лерді қосуға қатысты тапсырманы орындаймыз.

00:03:19.400 --> 00:03:30.400

Бүгінгі дәрісіміздің екінші бөліміне де жеттік. Мұнда AWS Site-to-Site VPN сервисін толығырақ қарастырамыз.

00:03:30.400 --> 00:03:44.400

Бұл сервистің идеясы - VPN арнасын IPSec протоколын қолданып, Интернет арқылы өткізу және AWS бұлтындағы VPC-ні бұлтта орналаспаған жергілікті желімен қосу.

00:03:44.400 --> 00:03:50.400

Бұл сервис үшін төлем әрбір қосылым үшін сағат сайын жүзеге асырылады.

00:03:50.400 --> 00:03:56.400

Бұл сервисте екі routing опциясы қолжетімді. Бұл - Dynamic routing және Static routing.

00:03:56.400 --> 00:04:06.400

Dynamic routing пайдаланған кезде құрылғылардың Border Gateway Protocol, яғни BGP протоколын қолдауы міндетті болып табылады.

00:04:06.400 --> 00:04:12.400

Егер бұл протоколға қолдау көрсетілмесе, екінші опция қалады, бұл - Static routing.

00:04:12.400 --> 00:04:22.400

Dynamic routing пен Static routing айырмашылығы неде? Dynamic Routing қосылым күйін тексеру үшін жергілікті қолдауға ие.

00:04:22.400 --> 00:04:29.400

Және резервтік арнаға сенімді қосқышты орната аласыз.

00:04:29.400 --> 00:04:35.400

Static routing туралы айтатын болсақ, оған жергілікті түрде қолдау көрсетілмейді, бірақ оны баптауға болады.

00:04:35.400 --> 00:04:43.400

Жергілікті желі AWS бұлтына қалай қосылады?

00:04:43.400 --> 00:04:52.400

AWS жағында Virtual Private gateway ресурсы және жергілікті желі жағында Customer gateway жасалады.

00:04:52.400 --> 00:04:59.400

Ол сәйкес жабдыққа бекітілген және олардың арасында VPN қосылымы бапталынады.

00:04:59.400 --> 00:05:07.400

Сондай-ақ, бір Virtual Private gateway-ге бірнеше Customer gateway қосуға болатынын атап өткен жөн.

00:05:07.400 --> 00:05:15.400

Осылайша, on-premise network жағында жоғары қолжетімділікті қамтамасыз етесіз.

00:05:15.400 --> 00:05:21.400

Осымен бүгінгі дәрісіміздің екінші бөлімін аяқтаймыз.

00:05:21.400 --> 00:05:23.400

Негізгі ойларды қарастырайық.

00:05:23.400 --> 00:05:39.400

Біріншісі, Интернет арқылы VPN қосылымын жасау арқылы жергілікті желіні AWS бұлт жағындағы VPC арқылы қосуға мүмкіндік беретін AWS Site-to-Site VPN сервисі бар.

00:05:39.400 --> 00:05:49.400

AWS Site-to-Site VPN құрылғыңыз қолдайтын протоколдарға байланысты екі routing опциясын қолдайды: Static және Dynamic.

00:05:49.400 --> 00:06:06.400

Үшіншісі, on-premise жағында бірнеше Customer gateway пайдалануға болады және осы қосылымдардың барлығын бір Virtual Private gateway-ге бағыттауға болады.

00:06:06.400 --> 00:06:16.400

Дәрісіміздің үшінші бөліміне жеттік және мұнда AWS Direct Connect сервисін толығырақ қарастырамыз.

00:06:16.400 --> 00:06:19.400

Қысқаша AWS DX деп атайды.

00:06:19.400 --> 00:06:27.400

Бұл сервистің идеясы да сондай, ол AWS бұлтымен жергілікті желіні қосуға көмектеседі, бірақ ол мұны басқаша жасайды.

00:06:27.400 --> 00:06:37.400

AWS Site-to-Site VPN сервисі туралы айтқан кезде, біз VPN арнасын интернет қосылымы арқылы жібердік.

00:06:37.400 --> 00:06:46.400

Ал егер сіздің интернет байланысыңыз сенімсіз немесе әлсіз болса, VPN осы шектеулер аясында жұмыс істейді.

00:06:46.400 --> 00:06:53.400

Интернет болмаса, бұлтқа дейінгі VPN қосылымы жоғалады.

00:06:53.400 --> 00:06:59.400

Direct Connect туралы айтатын болсақ, мұнда мүлдем басқа байланыс болады.

00:06:59.400 --> 00:07:10.400

Біз жаһандық AWS желісі және бүкіл әлемге таралған AWS серіктестері бар екенін білеміз.

00:07:10.400 --> 00:07:30.400

Және жаһандық AWS инфрақұрылымымен Direct Connect орнатқанда, олар үлкен мүмкіндіктер беретін Интернетке қатынаусыз өздерінің дата-центрлерін тікелей қосылыммен қамтамасыз етеді.

00:07:30.400 --> 00:07:46.400

Яғни, бұл қосылым жаһандық AWS инфрақұрылымы мен серіктестің дата-центрлерінде орналасқан ресурстар бір жергілікті желідегідей байланыса алатындығына сәйкес келеді.

00:07:46.400 --> 00:07:58.400

Және бұл сыйымдылығы жоғары арна жасауға мүмкіндік береді. Екі нұсқа ұсынылады. Бұл секундына 1 Гбит және секундына 10 Гбит.

00:07:58.400 --> 00:08:06.400

Сондай-ақ, Direct Connect арқылы қосылғанда Интернет қажет емес, яғни біз Интернетке тәуелсізбіз.

00:08:06.400 --> 00:08:11.400

Интернет өшіп қалса, AWS бұлтымен байланысыңыз сақталады.

00:08:11.400 --> 00:08:26.400

Осылайша, әртүрлі пайдалану жағдайлары үшін Direct Connect-ті пайдалану AWS Site-to-Site VPN-ге қарағанда қолайлырақ болуы мүмкін.

00:08:26.400 --> 00:08:37.400

Тағы бір маңызды жайт, Direct Connect сервисі жеке төленеді және AWS Site-to-Site VPN-нен бірнеше есе қымбат болуы мүмкін.

00:08:37.400 --> 00:08:48.400

Сондықтан барлық артықшылықтары мен кемшіліктерін талдағаннан кейін ғана AWS Direct Connect сервисіне ауысу туралы шешім қабылдау қажет.

00:08:48.400 --> 00:09:03.400

Қандай танымал қолдану жағдайлары бар? Біріншісі - гибридті инфрақұрылымдар, яғни сіздің инфрақұрылымыңыздың бір бөлігі жергілікті жерде, ал екінші бөлігі AWS бұлтында орналасқан кезде.

00:09:03.400 --> 00:09:13.400

Бұлтқа немесе жергілікті дата-центріне қайта көшуді жоспарламайсыз, осы режимде жұмысыңызды жалғастырасыз.

00:09:13.400 --> 00:09:26.400

Бұл жағдайда бұлт пен жергілікті инфрақұрылым арасында тасымалданатын ақпараттың айтарлықтай үлкен көлемі болуы мүмкін, сондықтан Direct Connect жақсы шешім болуы мүмкін.

00:09:26.400 --> 00:09:43.400

Басқа опция ақпараттың үлкен көлемі тасымалданған кезде, ал қалған екі опция бизнес тапсырмаңызға байланысты тұрақты байланысты қамтамасыз ету қажет болғанда.

00:09:43.400 --> 00:10:04.400

Сондай-ақ, кейбір құпия жеке деректерді Интернет арқылы тасымалдауға кедергі келтірмейтін кейбір нормативтік талаптар бар. Бұл жағдайда Direct Connect арқылы біз желіге кірмейміз және осы реттеу талаптарын бұзбаймыз.

00:10:04.400 --> 00:10:14.400

Осы диаграмманы мысал ретінде пайдалана отырып, енді AWS Direct Connect сервисі арқылы жергілікті инфрақұрылымды AWS бұлтына қосуды қарастырайық.

00:10:14.400 --> 00:10:49.400

Ортасында DX endpoint ресурсы орналасқан кейбір DX location көруге болады. Бұл DX endpoint бір жағынан жаһандық AWS инфрақұрылымына тікелей қосылады, екінші жағынан оған жергілікті дата-центрден DX endpoint-қа дейін жеке және жалпыға ортақ екі арна арқылы қосылу керек. Оны жасағаннан кейін DX endpoint арқылы кез келген AWS аймағындағы кез келген VPC-ге қосыла аласыз.

00:10:49.400 --> 00:11:01.400

Неліктен? DX endpoint жаһандық AWS инфрақұрылымына тікелей қосылатындықтан және барлық VPC-лер сонда орналасқандықтан, бұл мүмкіндік пайда болады.

00:11:01.400 --> 00:11:13.400

Сондай-ақ, DX endpoint арқылы Интернетке кіру кезінде осы кеңейтілген арна арқылы Amazon S3 сияқты жалпыға ортақ AWS сервистеріне қол жеткізуге болады.

00:11:13.400 --> 00:11:37.400

Неліктен бұл опция қызықты болуы мүмкін? Бұл дата-центрден Интернетке қосылу арнасының шағын болуына байланысты. Яғни, егер сіздің арнаңыз кішкентай болса, онда DX endpoint арқылы бұл арнаны кеңейтіп, көбірек ақпаратты жоғары жылдамдықпен жібере аласыз.

00:11:37.400 --> 00:12:19.400

Енді жергілікті дата-центр мен AWS бұлты арасындағы қолжетімділігі жоғары қосылымды жүзеге асырудың келесі мысалын қарастырайық. Бұл жағдайда AWS серіктесі арқылы AWS Direct Connect сервисін пайдалана отырып, жергілікті дата-центрін AWS бұлтына негізгі арна ретінде қостық және сақтық көшірме ретінде AWS Site-to-Site VPN сервисін қолдандық және VPN қосылымын интернет арқылы қостық. Мұнда Direct Connect жағдайында екі арна опциясы бар екенін еске салғым келеді. Бұл секундына 1 Гбит және секундына 10 Гбит.

00:12:19.400 --> 00:12:47.400

VPN арқылы қосылым десек, ол максималды 1,25 Гбит/с дейін жетуі мүмкін, сіздің интернет қосылымыңызға байланысты. Егер арнаның өзі соншалықты кең болмаса, онда сіз оны осы арнадан жылдам жібере алмайсыз. Бұл VPN қосылымының негізгі шектеуі.

00:12:47.400 --> 00:13:09.400

Басқа жағдайда, сіз халықаралық компания екеніңізді елестетіп көрейік, сізде қосымшаның бір бөлігі орнатылатын бірнеше дата-центр бар. Қолданбаңыздың басқа бөлігі AWS бұлтында орналасқан және қолданбаңыздың дұрыс жұмыс істеуі үшін бұлт пен жергілікті дата-центр арасында тұрақты байланыстарды қамтамасыз ету қажет.

00:13:09.400 --> 00:13:28.400

Бұл жағдайда әрбір дата-центріне AWS Direct Connect арқылы AWS бұлтына қосылымды баптау ұсынылады. Осылайша, дата-центрдің бірі істен шықса, сізде жеткілікті кең арна, AWS бұлтына тікелей қосылым болады және қолданба жұмысын жалғастырады.

00:13:28.400 --> 00:13:44.400

Бүгінгі дәрісіміздің үшінші бөлімін де аяқтадық. Ең маңызды сәттерді еске түсірейік. Біріншісі, AWS Direct Connect жаһандық AWS инфрақұрылымына тікелей қосылу үшін ашық стандарттарды пайдаланады.

00:13:44.400 --> 00:14:04.400

AWS Direct Connect арқылы қосылу кезінде сізде кез келген AWS аймағында орналасқан кез келген VPC, кез келген қоғамдық AWS сервисіне тікелей қол жеткізу мүмкіндігі бар. Себебі барлық AWS ресурстары бір жаһандық инфрақұрылымда орналасқан.

00:14:04.400 --> 00:14:20.400

Сондықтан, оған бір рет қосылсаңыз, барлық ресурстарға қол жеткізе аласыз. Сондай-ақ, жергілікті дата-центрден AWS бұлтына жоғары қолжетімді қосылымды орнатудың екі мысалын қарастырдық.

00:14:20.400 --> 00:14:35.400

Бірінші жағдайда Direct Connect және VPN қосылымы сақтық көшірме ретінде пайдаланылады, ал екінші жағдайда дата-центрдің әрқайсысы үшін Direct Connect пайдалану ұсынылады. Бұл қолданбаларыңыздың жоғары қолжетімділігін қамтамасыз етеді.

00:14:35.400 --> 00:14:55.400

Бірақ бұл жерде Direct Connect сервисі AWS Site-to-Site VPN-ге қарағанда бірнеше есе қымбатқа түсетінін еске салғым келеді, сондықтан сіз талдап, егер осы сервиске қанағаттансаңыз, оны қосылу үшін пайдалануыңызға болады.

00:14:55.400 --> 00:15:08.400

Біз дәрісіміздің төртінші бөліміне жеттік және мұнда VPC Peering функциясын пайдаланып бұлттағы VPC және AWS-ті бір-біріне қосуды егжей-тегжейлі қарастырамыз.

00:15:08.400 --> 00:15:48.400

Бір жағдайды елестетіп көрейік, сізде қолданба бар, ол дамып жатыр және сіздің барлық орталарыңыз бір VPC ішінде болған. Бірақ қолданбаңыз дамыған сайын көбірек ресурстар жасалады, көбірек AWS шектеулері болады, сондықтан әртүрлі жұмыс жүктемелерін бір-бірінен оқшаулау және басқару тұрғысынан логикалық шешім ретінде сіз әртүрлі VPC жасайсыз және әр ортаға арнайы VPC байланыстырасыз.

00:15:48.400 --> 00:15:55.400

Яғни, бір VPC-де Dev ортасы, басқа VPC-де сынақ ортасы, ал соңғысында негізгі Production орта болады.

00:15:55.400 --> 00:16:08.400

Бірақ әртүрлі факторларға байланысты белгілі бір тапсырмаларды орындау үшін бір ортадан екіншісіне қосылу керек.

00:16:08.400 --> 00:16:18.400

Және бұл жағдайда VPC Peering функциясы бізге көмекке келеді, бұл бір VPC-ді басқа VPC-ге тікелей қосуға мүмкіндік береді.

00:16:18.400 --> 00:16:23.400

Бұл жағдайда VPN қосылымдары жасалмайды, gateway жасаудың қажеті жоқ.

00:16:23.400 --> 00:16:40.400

Неліктен? Өйткені VPC екеуі де жаһандық AWS инфрақұрылымында орналасқан және сіз бір корпоративтік желідегі екі жергілікті желіні жергілікті желі арқылы бір-біріне қосасыз.

00:16:40.400 --> 00:16:54.400

Және бұл жағдайда Интернетке қосылым жоқ, сіз сол жаһандық желіде қаласыз, және қосылымның өзі де үлкенірек арнаға ие, сіз көбірек деректерді жоғары жылдамдықпен тасымалдай аласыз.

00:16:54.400 --> 00:17:09.400

Осылайша, осы қосылым арқылы сіз жеке IP мекенжайларының кеңістігінде қаласыз және жалпыға ортақ IP мекенжайларымен жұмыс істеудің қажеті жоқ.

00:17:09.400 --> 00:17:18.400

VPC Peering арқылы екі VPC қалай қосылғанын көру үшін осы диаграмманың мысалын қарастырайық.

00:17:18.400 --> 00:17:35.400

Ең бірінші - Peering Connection жасау, бұл қандай да бір ресурс. Ол қалай құрылады? AWS Management Console жағында сіз Peering connection жасайсыз және Peering қызметіне қосылу сұрауын жасайтын VPC көрсетесіз.

00:17:35.400 --> 00:17:51.400

Екінші VPC ретінде қосқыңыз келетін VPC көрсетіңіз. Бұл жерде VPC Peering көмегімен бір аймақта ғана емес, сонымен қатар әртүрлі аймақтарда орналасқан әртүрлі VPC-лерді бір-біріне қосуға болатынын ерекше атап өткім келеді.

00:17:51.400 --> 00:18:00.400

Сонымен қатар, VPC-ді бір-біріне тек бір AWS аккаунтында ғана емес, сонымен қатар басқа AWS аккаунтындағы VPC-ге де қосуға болады.

00:18:00.400 --> 00:18:09.400

Ең маңыздысы, Peering connection жасалғанда, сәйкес VPC-ге қосылуға шақыру жіберіледі.

00:18:09.400 --> 00:18:16.400

Егер ол бір AWS аккаунтында болса, шақыруды сол AWS Management Console-де көресіз.

00:18:16.400 --> 00:18:22.400

Оны қабылдағаннан кейін, Peering connection жасалады және екі VPC бір-біріне қосылады.

00:18:22.400 --> 00:18:35.400

Екінші VPC басқа AWS аккаунтында орналасса, сізде осы аккаунтқа кіру рұқсаты болуы керек немесе осы AWS аккаунтының иесі шақыруды қабылдайтыны туралы келісім болуы керек.

00:18:35.400 --> 00:18:46.400

Мұны істегеннен кейін, бірнеше қосымша қадамдар қалады. Бұл - Route tables.

00:18:46.400 --> 00:18:58.400

Бір жағдайды елестетіп көрейік, бізде VPC A бар және оның 10.1.0.0 CIDR блогы бар және өлшемі 16.

00:18:58.400 --> 00:19:09.400

Тағы бір жағдай, бізде VPC B бар және оның CIDR блогы 10.2.0.0 және өлшемі 16. Бұл 65000 мекенжай.

00:19:09.400 --> 00:19:34.400

VPC A жүйесінен VPC B ресурстарын көре алу үшін VPC A-мен байланысты Route Table-де қосымша routing rule тіркеу керек, мұнда Destination ретінде VPC B CIDR блогын және Target ретінде Peering Connection Resource көрсетесіз.

00:19:34.400 --> 00:19:42.400

Яғни, осы Peering Connection Resource арқылы VPC B CIDR блогындағы ресурстарға өтесіз.

00:19:42.400 --> 00:19:47.400

Тура солай, бірақ керісінше, VPC B жағынан жасайсыз.

00:19:47.400 --> 00:20:06.400

Онда Route Table үшін қосымша Routing rule тіркейсіз, мұнда Destination ретінде VPC A CIDR блогынжәне Target ретінде сол Peering Connection Resource, яғни PCX-1 көрсетесіз.

00:20:06.400 --> 00:20:12.400

Бірнеше VPC бір-біріне қосқанда, есте сақтау керек кейбір шектеулер бар.

00:20:12.400 --> 00:20:18.400

Біз жеке IP мекенжайлары кеңістігінде жұмыс істейміз.

00:20:18.400 --> 00:20:28.400

Екіншісі, біз әртүрлі аймақтарда және әртүрлі AWS аккаунтарында орналасқан VPC-ларды қоса аламыз.

00:20:28.400 --> 00:20:35.400

Тағы бір өте маңызды мәселе - VPC CIDR блоктары бір-біріменқиылыспауы керек.

00:20:35.400 --> 00:20:42.400

Егер олар қиылысса, олардың арасында VPC Peering теңшеу мүмкін болмайды.

00:20:42.400 --> 00:20:47.400

Бірнеше VPC арасында тек бірPeering Resource жасай аласыз.

00:20:47.400 --> 00:20:55.400

Яғни, біріншімен ақаулық туындаған жағдайда трафик сақтық көшірме арқылы өтетіндей етіп, сақтық Peering Resource жасау мүмкін болмайды.

00:20:55.400 --> 00:21:13.400

Шындығында, бұл тіпті қажет емес, өйткені Peering Connection Resource AWS жаһандық инфрақұрылымының жағында жасалған және оның ішінде жоғары қолжетімділік бар және оны ештеңемен қосымша өтеудің қажеті жоқ.

00:21:13.400 --> 00:21:27.400

Есте сақтау керек соңғы мәселе - VPC Peering арқылы бірнеше VPC қосу кезінде ешқандай транзитивтік эффект жасалмайды.

00:21:27.400 --> 00:21:32.400

Яғни, сізде VPC A, VPC B және VPC C бар деп елестетіңіз.

00:21:32.400 --> 00:21:37.400

Әрі қарай, VPC A және VPC B арасында VPC Peering жасағаныңызды елестетіңіз.

00:21:37.400 --> 00:21:43.400

Содан кейін, VPC B және VPC C арасында VPC Peering қосылымын жасадық.

00:21:43.400 --> 00:21:52.400

Бұл VPC A-дан VPC C-де орналасқан ресурстарға қол жеткізе алатыныңызды білдірмейді.

00:21:52.400 --> 00:21:56.400

Яғни, бұл жерде транзитивті эффекті болмайды.

00:21:56.400 --> 00:22:14.400

VPC A-дан VPC C-дағы ресурстарға, және керісінше, қол жеткізу қажет болса, бұрын тізімдеген барлық шектеулерді ескере отырып, осы екі VPC арасында жаңа Peering Connection жасау керек.

00:22:14.400 --> 00:22:29.400

Бірнеше VPC-мен жұмыс істегенде, екі VPC арасында қажеттілік бар жерлерде ғана қосылым жасау керек екенін есте ұстаған жөн.

00:22:29.400 --> 00:22:48.400

Барлық VPC-лерді бір-біріне қосуға ұмтылсақ, Peering connection саны көп болып кетеді және оны басқару қиынға соғады.

00:22:48.400 --> 00:22:57.400

Тағы бір мәселе, біз архитектураны оңай масштабталатындай етіп құруымыз керек.

00:22:57.400 --> 00:23:07.400

VPC саны өсіп келе жатса және соған қарамастан оларды біріктіру қажет болған жағдайда, басқа арнайы жасалған сервистер бар.

00:23:07.400 --> 00:23:11.400

Олар туралы келесі бөлімдерде айтатын боламыз.

00:23:11.400 --> 00:23:15.400

Енді бір мысалды қарастырайық.

00:23:15.400 --> 00:23:23.400

Біз бірнеше аймақтарда жұмыс істегенде, біздің негізгі инфрақұрылымымыз А аймағында орналасқан.

00:23:23.400 --> 00:23:28.400

Әрі қарай, инфрақұрылымның бір бөлігі бар, В аймағында орналасқан DR деп елестетейік.

00:23:28.400 --> 00:23:32.400

Ал негізгі аймақта бізде бірнеше түрлі VPC бар.

00:23:32.400 --> 00:23:38.400

VPC-лердің бірінде бізде Shared resources бар.

00:23:38.400 --> 00:23:50.400

Бұл кез келген нәрсе болуы мүмкін, қолданбалы модуль немесе ол, мысалы, корпоративтік желідегі барлық пайдаланушылар тіркелгілері үшін ақпаратты сақтайтын Active Directory болуы мүмкін.

00:23:50.400 --> 00:23:58.400

Және бұл жағдайда, бұл көптеген VPC қосылуы қажет VPC.

00:23:58.400 --> 00:24:01.400

Бұл диаграммада мысалды көресіз.

00:24:01.400 --> 00:24:13.400

Internal application-ге қызмет көрсететін VPC-леріміздің VPC Peering арқылы ортақ VPC-ге тікелей қосылғанын көреміз.

00:24:13.400 --> 00:24:20.400

Бұл VPC-ге қосылудың қажеті жоқ жағдайлар үшін ол бапталмаған.

00:24:20.400 --> 00:24:32.400

Сондай-ақ, VPN қосылымы жергілікті дата-центрден shared VPC-ге VPN веб-сайты арқылы бапталғанын көресіз.

00:24:32.400 --> 00:24:37.400

Осымен бүгінгі дәрісіміздің төртінші бөлімін аяқтадық.

00:24:37.400 --> 00:24:40.400

Тоқтап, ең маңызды сәттерді еске түсірейік.

00:24:40.400 --> 00:24:48.400

VPC Peering – бұл екі бөлек VPC бір-біріне тікелей қосуға мүмкіндік беретін ресурс, функционал.

00:24:48.400 --> 00:24:55.400

Бұл VPC әртүрлі аймақтарда және әртүрлі AWS аккаунтарында орналасуы мүмкін.

00:24:55.400 --> 00:25:13.400

VPC Peering құру кезінде сұрауды жіберетін VPC Peering Connection жасайды және осы шақыруды қабылдайтын VPC екінші бөлігі осы шақыруды қабылдауы керек, содан кейін Peering Connection ресурсы іске қосылады.

00:25:13.400 --> 00:25:22.400

Әрі қарай, екі VPC арасындағы ресурстар ақпарат алмасуы үшін route table және мүмкін security топтарын баптауымыз керек.

00:25:22.400 --> 00:25:27.400

Peering Connection жасау кезінде белгілі шектеулер бар.

00:25:27.400 --> 00:25:41.400

Біз жеке IP мекенжайлары кеңістігінде жұмыс істейміз, яғни жалпыға ортақ IP мекенжайлары пайдаланылмайды, өйткені біз жаһандық AWS инфрақұрылымында қаламыз және Интернетке кірмейміз.

00:25:41.400 --> 00:25:49.400

Тағы бір мәселе, бірнеше VPC арасында қосылымды жасау кезінде CIDR блоктары бір-бірімен қиылыспауы керек.

00:25:49.400 --> 00:25:52.400

Егер олар қиылысса, онда Peering connection баптау мүмкін емес.

00:25:52.400 --> 00:26:06.400

Сондықтан, бұл туралы алдын ала ойлану керек және ұйым ішінде кез келген VPC жасағанда, оларды CIDR блоктары бастапқыда қиылыспайтындай етіп жасаңыз.

00:26:06.400 --> 00:26:11.400

Олар болашақта байланыспаса да, біз мұны алдын ала біле алмаймыз.

00:26:11.400 --> 00:26:20.400

VPC-ді барлық ресурстарымен бірге басқа VPC-ге ауыстырғаннан гөрі оны басында ескеру әлдеқайда арзан.

00:26:20.400 --> 00:26:23.400

Бұл компания үшін айтарлықтай уақыт пен шығындарды талап етеді.

00:26:26.400 --> 00:26:37.400

Екі VPC арасында бірнеше Peering connection баптау мүмкін емес, бірақ бұл тіпті қажет емес, өйткені Жоғары қолжетімділік Peering connection ішінде бұрыннан бар.

00:26:37.400 --> 00:26:44.400

Емтиханда сұрақ түрінде жиі келетін соңғы мәселе - транзитивті эффектісі.

00:26:44.400 --> 00:26:53.400

Егер біз VPC A-ді VPC B-мен, содан кейін VPC B-ді VPC C-мен қоссақ, онда VPC A және VPC C арасында ешқандай байланыс пайда болмайды.

00:26:53.400 --> 00:27:00.400

Егер оларды бір-біріне қосу қажет болса, осы екі VPC арасында нақты Peering Connection жасау керек.

00:27:03.400 --> 00:27:11.400

Біз дәрісіміздің бесінші бөліміне жеттік және AWS Transit Gateway сервисіне туралы толығырақ тоқталамыз.

00:27:11.400 --> 00:27:27.400

Бізде бірнеше VPC бар жағдайды елестетіп көрейік және біз әрбір VPC үшін инфрақұрылымымыздағы кез келген басқа VPC-ге қосылу мүмкіндігін қамтамасыз етуіміз керек.

00:27:27.400 --> 00:27:44.400

VPC Peering проблемасы мынада: VPC саны артқан сайын және барлық VPC арасында толық қосылымды қамтамасыз ету қажеттілігімен VPC Peering саны өте тез өседі.

00:27:44.400 --> 00:27:46.400

Бірге санап көрейік.

00:27:46.400 --> 00:27:50.400

Бізде екі VPC бар және оларды біріктіру керек деп елестетіп көрейік.

00:27:50.400 --> 00:27:53.400

Бұл жағдайда біз бірPeering connection жасаймыз.

00:27:53.400 --> 00:28:12.400

Әрі қарай, егер VPC санын біреуге көбейтсек және ол үшке тең болса, бұл жағдайда үш VPC Peering connection жасау қажет, яғни бірінші мен екінші, екінші және үшінші, сондай-ақ үшінші мен бірінші арасында, өйткені транзитивтілікке қолдау көрсетілмейді.

00:28:12.400 --> 00:28:25.400

Егер біз төрт VPC туралы айтатын болсақ, онда бұл жағдайда барлық VPC-лерді бір-біріне қосу үшін 6 Peering connection қажет болады.

00:28:25.400 --> 00:28:39.400

Егер бес VPC болса, онда бұл жағдайда бізге 15 Peering connection қажет болады.

00:28:39.400 --> 00:28:44.400

Сіз VPC Peering қажетті саны қаншалықты жылдам өсіп жатқанын көресіз.

00:28:44.400 --> 00:28:57.400

Бұл нақты істі басқаруды жеңілдету үшін арнайы шешім әзірленді.

00:28:57.400 --> 00:29:01.400

Бұл - AWS Transit Gateway сервисі.

00:29:01.400 --> 00:29:28.400

Идея мынада: VPC немесе жергілікті дата-центрден VPN қосылымы немесе Direct Connect Gateway түрінде қосылым болсын, содан кейін AWS Transit Gateway желісіне қосылған кезде, барлық бар қосылымдар жаңа қосылымдарға қолжетімді болады.

00:29:28.400 --> 00:29:48.400

Яғни, бұл жағдайда сіз мысалда алты түрлі қосылымды көресіз және бізге 15-тен астам Peering connection жасаудың қажеті болмады, бірақ AWS Transit Gateway-ге әрбір VPC үшін бір қосылым жасау жеткілікті.

00:29:48.400 --> 00:30:00.400

Осылайша, әрбір VPC осы Transit gateway-дегі кез келген басқа қосылымдарға қосыла алды.

00:30:00.400 --> 00:30:03.400

Енді бұл сервистің не екендігі туралы толығырақ сөйлесейік.

00:30:03.400 --> 00:30:17.400

AWS Transit Gateway — көптеген желілік қосылымдарды біріктіруді жеңілдететін желілік сервис.

00:30:17.400 --> 00:30:29.400

Ол орталық хаб ретінде жұмыс істейді және оған қосылатын барлық қосылымдар барлық басқа қосылған ресурстарға қолжеткізе алады.

00:30:29.400 --> 00:30:40.400

Бір AWS Transit Gateway-ге 5000-ғадейінәртүрліқосылымдардықосуғаболады.

00:30:40.400 --> 00:30:54.400

Transit Gateway үшін, сондай-ақ AWS Site-to-Site VPN сервисі үшінбелгілібіршектеулер, кемшіліктерменартықшылықтарбарекенінатапөткімкеледі.

00:30:54.400 --> 00:30:56.400

Олар, сондай-ақ, бағасыбойыншаерекшеленеді.

00:30:56.400 --> 00:31:11.400

Сондықтан, сіздің бизнес-кейсіңізге байланысты, сізосытармақтардыңбарлығын, атапайтқанда, архитектурағақатыстыаспектілерді, сондай-ақ, төлеммәселелерінескеруіңізкерек.

00:31:11.400 --> 00:31:20.400

Transit Gateway сізүшінтиімдішешімемесекенібелгіліболуымүмкін, ондай жағдайда VPC Peering Connection сервисінде қалуыңызкерек.

00:31:20.400 --> 00:31:42.400

Немесе керісінше жағдайда, VPC Peering connection сізге сәйкес келмейді, өйткені қосылымдар саны өсіп келеді және бұл тиімсіз және Transit Gateway осы қосылымдардың барлығын басқаруды жеңілдетіп қана қоймай, сонымен қатар үнемді болуы мүмкін.

00:31:42.400 --> 00:31:50.400

AWS Transit Gateway қалай бапталынатынын жақсырақ түсіну үшін келесі мысалды қарастырайық.

00:31:50.400 --> 00:31:53.400

Бізде келесі CIDR блоктары бар 3 VPC бар.

00:31:53.400 --> 00:32:01.400

Олардың барлығын Peering connection қолданбай, Transit gateway арқылы қосуымыз керек.

00:32:01.400 --> 00:32:05.400

Бірінші кезекте AWS Transit Gateway ресурсын жасау керек.

00:32:05.400 --> 00:32:12.400

Әрі қарай, әрбір VPC жағында ENI, яғни Elastic Network Interface баптау керек.

00:32:12.400 --> 00:32:17.400

Осы ресурс арқылы VPC-ге қосылу жүзеге асырылады.

00:32:17.400 --> 00:32:32.400

Біз оны route table-ге қосамыз, яғни әрбір VPC бапталған әдепкі route table-ге ие, ол белгілі бір VPC ішіндегі барлық ресурстар арасындағы трафикке мүмкіндік береді.

00:32:32.400 --> 00:32:37.400

Енді Route Table әрқайсысына өзгертулер енгізуіміз керек.

00:32:37.400 --> 00:32:50.400

Үшінші VPC мысалында, Destination ретінде барлық үш VPC CIDR блоктарын қамтитынCIDRблогын және Target ретінде Transit gateway көрсеткенімізді көреміз.

00:32:50.400 --> 00:32:58.400

Келесі қадам Transit gateway жағында route table баптау болып табылады.

00:32:58.400 --> 00:33:13.400

Және бұл жерде әрбір VPC үшін Destination ретінде сәйкес VPC-дің Target Elastic Network Interface бар route көрсететінімізді көрсетеміз.

00:33:13.400 --> 00:33:27.400

Содан кейін трафик Transit Gateway-ге жеткенде, Transit GatewayRoute Table-дегі ережеге негізделген трафик қайда бағытталғанын және қандай Target пайдалану керектігін қарайды.

00:33:27.400 --> 00:33:55.400

VPC 3-тен бірінші VPC CIDR блогындағы ресурстарға қол жеткізіп жатырмыз деп елестетіп көрейік, онда ол IP мекенжайын қарайды және үшінші VPC-дің жағында route көреді, олTarget ретінде Transit Gateway қолданады және осы CIDR блогына қатынайды дегенді білдіреді.

00:33:55.400 --> 00:33:59.400

Осыдан кейін трафик Transit Gateway жағына өтеді.

00:33:59.400 --> 00:34:10.400

Transit Gateway сонымен қатар өзінің Route Table қарайды және біз қатынасатын IP мекенжайы бірінші VPC-ге тиесілі екенін көреді.

00:34:10.400 --> 00:34:35.400

Ал трафикті бірінші VPC-ге бағыттау үшін біз сәйкес Elastic Network Interface пайдалануымыз керек және сәйкесінше бұл трафикті осы ресурсқа бағыттауымыз керек. Осыдан кейін бұл трафикті VPC 1 жағында көруге болады, яғни қосылым іс жүзінде қамтамасыз етіледі.

00:34:35.400 --> 00:34:38.400

Енді келесі жағдайды қарастырайық.

00:34:38.400 --> 00:34:42.400

Бізде жергілікті дата-центрден VPN connection бар.

00:34:42.400 --> 00:34:59.400

Бірінші нұсқа - VPC бір-бірімен қиылыспайтындай әрбір VPC-ден жергілікті дата-центрдегі ресурстарға оқшауланған қосылымды қамтамасыз ету.

00:34:59.400 --> 00:35:17.400

Бұл жағдайда бізге Transit Gateway-де Route Table-ді өзгерту керек және Destination ретінде бүкіл Интернеттің немесе белгілі бір CIDR блогының белгіленуі және бұл трафикті VPN-ге бағыттау керек.

00:35:17.400 --> 00:35:32.400

Осылайша, трафик ретінде бірінші VPC-дің IP мекенжайын көрсетсеңіз де, ол route rule-ге сәйкес оны VPN-ге бағыттайды.

00:35:32.400 --> 00:35:39.400

Әртүрлі VPC-де орналасқан ресурстар бір-бірімен трафикті алмастыра алмайды.

00:35:39.400 --> 00:35:45.400

Бірақ сонымен бірге олар VPN арқылы трафикті жергілікті дата-центрлерге жібере алады.

00:35:45.400 --> 00:36:03.400

Келесі жағдай - AWS ішінде қалған, бірақ басқа VPC-ге өтетін, және басқа трафик VPN-ге бағытталуы үшін барлық трафикті сақтау қажет болғанда.

00:36:03.400 --> 00:36:14.400

Бұл жағдайда біз Transit gateway-де Route table-ді өзгерте аламыз немесе алдыңғы routes көрсетілетін басқа Route Table қоса аламыз.

00:36:14.400 --> 00:36:29.400

Осылайша, біз үшінші VPC-ден, мысалы, екінші VPC-дегі ресурстарға қол жеткізгіміз келгенде, екінші route table-ге сәйкес, біз трафикті сәтті бағыттаймыз.

00:36:29.400 --> 00:36:49.400

Әрі қарай, егер біз трафигімізді VPC-ге емес, басқа IP мекенжайына бағыттағымыз келсе, ол екінші route table-ге қатысты ережелерге сәйкес келмейді және бірінші route table-ді қарастырады, бұл трафикті VPN жағына бағыттау керек екенін көреді және сәйкесінше бұл трафик сол жерге барады.

00:36:53.400 --> 00:37:01.400

AWS Transit Gateway жағдайында оны қалай баптау керектігін есте сақтау үшін шағын тапсырманы орындайық.

00:37:01.400 --> 00:37:09.400

Осы тапсырманың аясында бізге қиылыспайтын бірегей CIDR блогы бар 5 түрлі VPC беріледі.

00:37:09.400 --> 00:37:18.400

Бізде сондай-ақ Transit Gateway бар және біз барлық VPC-лерді AWS Transit Gateway арқылы бір-біріне толығымен қосуымыз керек.

00:37:18.400 --> 00:37:28.400

Әрбір VPC-дің Route Table деңгейінде қандай әрекеттерді орындау керек және Transit Gateway Route table деңгейінде қандай әрекеттерді орындау қажет?

00:37:28.400 --> 00:37:32.400

Сіз бұл видеоны тоқтатып, өзіңіз жауап беруге тырысыңыз.

00:37:37.400 --> 00:37:43.400

Жақсы, дұрыс жауап бере алдыңыз деп ойлаймын, енді не істеу керек екенін тексерейік.

00:37:43.400 --> 00:37:49.400

Ең алдымен, әрбір VPC деңгейінде бізге бір route қосу керек.

00:37:49.400 --> 00:38:00.400

Бұл route Destination ретінде CIDR блогын қамтиды, бұл CIDR блогы барлық бар VPC құрылғыларының CIDR блоктарын қамтуы керек және Target ретінде Transit Gateway көрсетілуі керек.

00:38:00.400 --> 00:38:14.400

Осылайша, біз Route Table жағында әдепкі бірінші route осы VPC CIDR блогын қамтитынын және Target ретінде local көрсететінін есте ұстаймыз.

00:38:14.400 --> 00:38:33.400

Бұл трафик жіберілетін IP мекенжайы белгілі бір VPC-нің CIDR блогына жататын болса, онда ол жергілікті трафик ретінде танылады және сәйкесінше сол VPC-де орналасқан ресурсқа бағытталады.

00:38:33.400 --> 00:38:39.400

Яғни, бұл VPC ішіндегі барлық ресурстарға бір-бірімен байланысуға мүмкіндік беретін route.

00:38:39.400 --> 00:39:07.400

Енді біз қосқан келесі route, ол барлық басқа CIDR блоктарын қамтиды және егер бізде белгілі бір VPC CIDR блогына жатпайтын, бірақ сыртқа шығатын IP мекенжайына сұрау болса, онда бұл жағдайда оның жалпыCIDRблогынажататынын тексереміз.

00:39:07.400 --> 00:39:10.400

Олай болса, бұл трафик Transit Gateway-ге өтеді.

00:39:10.400 --> 00:39:13.400

Мұндай өзгерістер әрбір VPC деңгейінде жасалуы керек.

00:39:13.400 --> 00:39:23.400

Енді біз Transit Gateway туралы айтатын болсақ, мұнда route table-ге 5 route, әрбір VPC үшін 1 route қосу керек.

00:39:23.400 --> 00:39:25.400

Бұл route келесі параметрлерді қамтиды.

00:39:25.400 --> 00:39:34.400

Destination ретінде VPC CIDR блогын көрсетеміз, ал Target ретінде сол VPC Elastic Network Interface көрсетеміз.

00:39:34.400 --> 00:39:55.400

Яғни, егер Transit Gateway-де белгілі бір IP мекенжайына бағытталған трафикті алсақ, ол оның барлық route-тарын тексереді және егер бұл IP мекенжай Destination-дағы CIDR блоктарының біріне жататын болса, онда ол трафикті осы Target-ке бағыттайды.

00:39:55.400 --> 00:40:07.400

Осылайша, біз Transit Gateway арқылы барлық VPC арасындағы байланысты баптай алдық.

00:40:07.400 --> 00:40:16.400

Осымен бесінші бөлім аяқталды және мұнда AWS Transit Gateway сервисіне қатысты негізгі ойларды атап өтуге болады.

00:40:16.400 --> 00:40:25.400

AWS Transit Gateway VPC Peering connection бірдей рөл атқарады, бірақ оның орталық хаб болуымен ерекшеленеді.

00:40:25.400 --> 00:40:44.400

Peering connection жағдайында біз екі VPC-ді бір-біріне тікелей қосамыз, ал Transit Gateway жағдайында бізге VPC-ні Transit Gateway-ге қосу жеткілікті және ол осы Transit Gateway-ге қосылған барлық қолданыстағы қосылымдарға қол жеткізе алады.

00:40:44.400 --> 00:40:54.400

Сіздің бизнес жағдайыңызға немесе мәселеңізге байланысты сізге қайсысытиімді екенін шешу керек.

00:40:54.400 --> 00:41:16.400

Немесе VPC арасында қосылымдар саны аз болған жағдайда VPC Peering connection пайдаланыңыз, ал керісінше жағдайда, VPC саны көп болса және әрбір VPC әрбір басқа VPC-ге қосылуы қажет болса, онда бұл жағдайда сізге қолайлы шешім AWS Transit Gateway болуы мүмкін.

00:41:16.400 --> 00:41:33.400

Біз дәрісіміздің алтыншы және соңғы бөліміне жеттік және мұнда VPC ресурстарына басқа AWS сервистеріне қол жеткізуге мүмкіндік беретін ресурстар туралы айтатын боламыз.

00:41:33.400 --> 00:41:38.400

Мұны жүзеге асыру үшін VPC Endpoints пайдалану ұсынылады.

00:41:38.400 --> 00:41:55.400

Бұл - VPC ресурстарына желіге қосылмай және жаһандық AWS инфрақұрылымында қалмай AWS сервистеріне тікелей қосылуға мүмкіндік беретін ресурс.

00:41:55.400 --> 00:42:03.400

Осылайша, бізге Internet Gateway, VPN қосылымы, NAT Gateway және т.б. баптаудың қажеті жоқ.

00:42:03.400 --> 00:42:10.400

VPC Endpoints қосудың екі нұсқасы бар.

00:42:10.400 --> 00:42:25.400

Біріншісі - Interface Endpoint, бізге жеке IP мекенжайы бөлінген кезде және осы жеке IP мекенжайы арқылы AWS Private Link функциясын пайдалана отырып, біз басқа сервистерге қосыламыз.

00:42:25.400 --> 00:42:32.400

Барлық сервистер қолжетімді емес. Бұл сервистердің мысалдары Amazon CloudWatch, Amazon EC2 және Elastic Cloud Balancing болып табылады.

00:42:32.400 --> 00:42:35.400

Екінші опция - Gateway Endpoint.

00:42:35.400 --> 00:42:44.400

Бұл жағдайда белгілі бір трафикті AWS қолдайтын сервистерге бағыттау үшін route table жағында өзгерістер енгізіледі.

00:42:44.400 --> 00:42:49.400

Бұл жағдайда мысалдары Amazon S3 және DynamoDB болып табылады.

00:42:49.400 --> 00:42:56.400

Енді Interface Endpoint параметрін баптауға болатын мысалдарды қарастырайық.

00:42:56.400 --> 00:43:06.400

Ең алдымен, біз қандай сервиспен жұмыс істейтінімізді және бұл сервиске Interface Endpoint арқылы қолдау көрсетілетінін шешуіміз керек.

00:43:06.400 --> 00:43:15.400

Қолдау көрсетілсе, біз VPC туралы шешім қабылдауымыз керек, ресурстардың осы сервиске қосылатын subnet анықтауымыз керек.

00:43:15.400 --> 00:43:20.400

Төртінші қадамда жеке DNS әдепкі бойынша белсендіруге болатынын көресіз.

00:43:20.400 --> 00:43:22.400

Мұның не үшін қажет екенін сәл кейінірек айтамын.

00:43:22.400 --> 00:43:32.400

Соңғы қадам - ​Network Interface үшін қажетті security groups баптау.

00:43:32.400 --> 00:43:41.400

Енді мұның бәрі өзара әрекеттесетін мысалдарды қарастырайық.

00:43:41.400 --> 00:43:56.400

Біз VPC-ден белгілі бір сервиске қосылымды орнатқан кезде, ол Amazon Kinesis Data Streams болсын, біз оған default DNS hostname арқылы қол жеткізе аламыз.

00:43:56.400 --> 00:44:11.400

Бұл сервистің URL мекенжайы, ол арқылы біз осы сервиске қол жеткізе аламыз, бірақ мәселе мынада, бұл кіру Internet gateway арқылы, Интернет арқылы өтеді және сіз қосымша параметрмен қажетін көрсетесіз.

00:44:11.400 --> 00:44:15.400

Кейбір жүктемелер үшін бұл мүмкін емес.

00:44:15.400 --> 00:44:19.400

Басқа нұсқа бар. Endpoint Specific DNS hostname пайдалануға болады.

00:44:19.400 --> 00:44:27.400

Бұл Interface Endpoint-ке кейбір DNS hostname тағайындалған кезде.

00:44:27.400 --> 00:44:33.400

Басқаша айтқанда, бұл URL мекенжайына сұраныс бойынша трафик сізге қажет сервиске бағытталады.

00:44:33.400 --> 00:44:37.400

Сонымен, бұл жағдайда Private DNS қосылмаған.

00:44:37.400 --> 00:44:42.400

Сонымен, егер біз бұл сервиске қол жеткізгіміз келсе, бізде екі нұсқа бар.

00:44:42.400 --> 00:44:50.400

Default DNS hostname арқылы қол жеткізілсе, трафик Internet gateway арқылы өтеді және Интернет арқылы біздің сервисімізге жетеді.

00:44:50.400 --> 00:45:06.400

Немесе Amazon Kinesis Data Stream қосылымымен Interface Endpoint ішінде жасалған қолданбаларымыздың жағында ерекше бірегей URL мекенжайын нақты көрсетуіміз керек.

00:45:06.400 --> 00:45:20.400

Бұл URL мекенжайына сұрау ғаламдық AWS инфрақұрылымында орын алады, Интернетке өтпейді және VPC ішіндегі ресурстар нақты сервиске тікелей қол жеткізеді.

00:45:20.400 --> 00:45:54.400

Енді тағы бір жағдай бар, біз Private DNS іске қосқан кезде, бұл жағдайда трафикті Интернет арқылы, Internet gateway арқылы әдепкі DNS hostname-ге бағыттаудың қажеті жоқ және бұл әдепкі DNS hostname да белсенді болып қалады, бірақ осы URL мекенжайына сұрау арқылы біз трафикті Interface Gateway арқылы қажетті сервиске бағыттаймыз.

00:45:54.400 --> 00:46:04.400

Басқаша айтқанда, біз әрбір сервис үшін әдепкі DNS hostname білеміз, ол өзгермейді, ол стандартты.

00:46:04.400 --> 00:46:39.400

Сонымен, егер біз оны пайдаланғымыз келсе, бұл өте ыңғайлы, біз Private DNS опциясын қоса аламыз және осылайша VPC ішіндегі қолданбаларымыз үшін орта айнымалыларында Endpoint Specific DNS hostname қосымша көрсетудің қажеті жоқ, бірақ белгілі бір сервистің жалпыға қолжетімді URL мекенжайын, оның ғаламдық AWS инфрақұрылымында және Интернетке қосылусыз Interface Endpoint арқылы өтетінін біле отырып, оған тікелей қол жеткізе аласыз.

00:46:39.400 --> 00:46:53.400

Жақсы, осылайша біз дәрісіміздің алтыншы бөлімінің соңына жеттік, бізде VPC ресурстарының AWS сервистеріне қосылу мүмкіндігі бар екенін көрдік.

00:46:53.400 --> 00:47:01.400

Екі нұсқа бар. Бірінші нұсқа -Interface Gateway арқылы, ал екіншісі - Gateway Endpoint арқылы.

00:47:01.400 --> 00:47:18.400

Екі жағдайда да, сізге қандай сервис қажет екеніне байланысты белгілі бір AWS сервистеріне қолдау көрсетіледі және қолдау көрсетілетін сервистер тізімін қарап, қай опцияны қолдану керектігін түсінуге болады.

00:47:21.400 --> 00:47:25.400

Осымен бүгінгі дәрісімізді аяқтаймыз.

00:47:25.400 --> 00:47:31.400

Біз networking-ке қатысты маңызды мәселелерді талқыладық.

00:47:31.400 --> 00:47:43.400

Жергілікті инфрақұрылымды AWS бұлттарымен қалай қосуға болатынын, бұл үшін қандай мүмкіндіктер бар екенін, кем дегенде екі нұсқаны қарастырдық.

00:47:43.400 --> 00:47:50.400

Біз сондай-ақ AWS бұлтында VPC, бірнеше VPC бір-біріне қосу опциясын қарастырдық.

00:47:50.400 --> 00:47:53.400

Сіздің жағдайыңызға байланысты да бірнеше нұсқа бар.

00:47:53.400 --> 00:48:10.400

Және соңғы нұсқа, біз сондай-ақ сервисті VPC ішінде орналастыру мүмкін емес, бірақ VPC-ден VPC Endpoint арқылы осы сервистермен қауіпсіз жұмыс істей алатын жағдайды қарастырдық.

00:48:13.400 --> 00:48:20.400

Бұл слайдта сіз Интернеттегі қосымша ресурстарға қол жеткізуге көмектесетін кілт сөздерді көре аласыз.

00:48:20.400 --> 00:48:32.400

Көбінесе олар AWS құжаттамасын немесе YouTube видео хостинг сайтында орналасқан re:Invent жазбаларын жүргізеді.

00:48:34.400 --> 00:48:37.400

Осымен бүгінгі дәрісіміз аяқталды.

00:48:37.400 --> 00:48:44.400

Назарларыңызға рахмет, келесі белсенділіктерде кездескенше.