Қайырлы күн, құрметті студенттер! Сіздерді көргеніме қуаныштымын! Кезекті Демо-сессияға қош келдіңіздер! Біз бүгін AWS Identity and Access Management сервисі (IAM) туралы толығырақ айтамыз. Сіздер бұл сервисті көбінесе AWS IAM деп кездестірулеріңіз мүмкін. Сонымен, бастайық.

AWS Management Console-ге тіркелген соң, негізгі парақшаға өтеміз. Оcы жерден Демоны бастаймыз. Бізге AWS IAM сервисінің негізгі парақшасына өту керек болады. Ол үшін AWS-тің арнайы сервисті іздеу жолына IAM деп жаза бастаймыз. Бірінші болып бізге керек сілтеменің шыққанын көресіздер. Енді, сервистің негізгі парақшасына өту үшін осыған басайық. Біз өзімізге керек парақшаға өттік. Сіздер сол жақта біздің IAM Dashboard қойындысында екенімізді көрдіңіздер. Бұл парақшадан не көре алатынымызды толығырақ қарап шығайық.

Ең бірінші блок – Security recommendations. Бұл сіздің AWS аккаунтыңызды қауіпсіз қылу үшін жасалатын тапсырмалар тізімі. Тізім сіздің Root қолданушы немесе ІAМ User ретінде тіркелгеніңізге байланысты ерекшеленуі мүмкін. Мұнда орындалған тапсырмалар жасыл түспен белгіленген, ал орындалуы тиіс тапсырмалар қызылмен белгіленеді.

Келесі блок – IAM Resources. Бұл блокта сізде қандай да бір нақты ресурстың нешеуі бар екенін білесіз. Мысалы, аталған аккаунтта 1 User group, 1 User, 17 Roles, 5 Polices және 1 Identity provider бар.

Сіздерге көрсеткім келген келесі блок – AWS account. Бұл блокта не бар екенін көрелік. Ең бірінші сіздер Account ID-ді көрулеріңіз мүмкін. Бұл – сіздің аккаунтыңыздың құрылуы кезінде берілетін аккаунттың бірегей идентификаторы. Оны тез көшіріп алуға мүмкіндік беретін арнайы батырма бар. Екінші, Account Alias аккаунтының баптауларын көресіздер. Әр аккаунт үшін аккаунтыңызды анықтау жеңіл болу үшін осы жерде Alias-ті баптауға болады. Alias-ті орнатқаннан кейін, сіздің Sign-in URL, яғни IAM қолданушы ретінде тіркелетін қызметкерлеріңізге берілетін URL өзгеріп, Account ID-дің орнына сіздің Account Alias орнатылады. Біз AWS IAM сервисінің негізгі парақшасында көрінетін басты блоктармен таныстық.

Ал енді AWS IAM-нің қандай ресурстары болатынын толығырақ қарастырайық. User groups-тан бастайық. Бұл аккаунттағы бар топтарды көрсету үшін сізге User groups қойындысына өту керек. Бұл аккаунтта admins деп аталатын жалғыз топ бар. Енді, жаңа топ құру үшін экранның жоғарғы оң жағындағы батырманы басайық. Бұл парақшада сізге жаңа топтың атын енгізу керек, сондай-ақ бұрыннан бар пайдаланушыларды осы жаңа топқа қосуға болады. Егер парақшаны сәл төмен айналдырсаңыз, бір немесе бірнеше бар Policies-тарды қоса алатыныңызды көресіз. Біз қосымша (Optional) жолдарды толтырмаймыз, сондықтан ең соңына дейін айналдырып, Create group батырмасын басамыз. Бұл батырманы басқан соң, сізді бар топтардың парақшасына жібереді. Сондай-ақ бұл парақшада жасыл түспен топтың сәтті құрылғаны жайлы хабарландыру шығып тұрады. Негізгі парақшада біз ашқан жаңа Students тобы басқа топтармен тізімде пайда болғанын көресіз.

Біз сіздермен AWS IAM-нің келесі ресурсы – IAM Users-ке өтеміз. Бар IAM қолданушылардың тізіміне өту үшін сіздерге Users қойындысына өту керек. Бұл AWS аккаунтта бір қолданушы Admin бар екенін көреміз. Енді, жаңа IAM қолданушысын құрып көрейік. Ол үшін бізге экранның оң жағындағы Add user батырмасын басу керек. IAM қолданушысын құруда бізге жаңа қолданушының баптаулары бар әртүрлі бес парақшадан өту керек. Барлық парақшаларды толтыру міндетті емес. Енді, әрқайсынан өтіп көрейік. Ең бірінші парақшада сізге қолданушының атын енгізу керек болады. Дәл осы парақшаның төмен жағында қолданушыға қандай қолжетімділік беруге болатынын таңдай аласыз. Ең бірінші блок – Access key - Programmatic access. Егер қолданушы AWS CLI-ді немесе AWS SDK-ді қолданған болса, яғни, бағдарламалық қолжетімділік керек болса, осыны белгілей аласыз. Ары қарай, егер сіздің қолданушыға AWS Management Console керек болса, онда сізге оны сәйкес белгімен белгілеу керек. Сондай-ақ сіз құпиясөздің баптауларын көрсете аласыз. Бұл генерацияланған құпиясөз, не өзіңіз құрастырған құпиясөз болуы мүмкін. Егер қолданушыға бірінші тіркеуден кейін құпиясөзді өзгерту керек болса, онда сізге ең соңғы пунктті белгілеу керек.

Жаңа қолданушыны құрудағы баптаудың екінші парақшасында бұл қолданушыға қандай құқық беретінімізді анықтап алғанымыз жөн. Оның 3 нұсқасы бар. Бірінші нұсқа: бұл қолданушыны бар топтың біреуіне қосу. Екінші нұсқа: бар қолданушының құқығы мен мүмкіндігін көшіріп алу. Үшінші нұсқа: бар Policies-терді осы қолданушыға бірден қосу. Біз қолданушыны бар топтың біреуіне қосатын бірінші нұсқаны таңдаймыз. Сіз осы опцияға басқанда, экранның төменгі жағында бар тіркелген топтың тізімі шығады. Енді, қолданушымызды жаңа ғана құрылған Students тобына қосайық. Одан кейін баптаулардың келесі парақшасына өту үшін next батырмасын басамыз.

Үшінші парақшада бізге жаңа қолданушымызға тегтер жазуымыз керек болады. Біз қолданушы да AWS-тің ресурсы екенін білеміз. Бұл парақша міндетті емес, сондықтан біз оны толтырмаймыз. Келесі парақшаға өту үшін next батырмасын басамыз.

Төртінші парақшада қолданушымызға арналған өзіңіз енгізген барлық баптауларды көре аласыз. Егер барлығы дұрыс, болса осы қолданушыны құру үшін create user батырмасын басамыз.

Қолданушыны құру баптауларының бесінші парақшасында қолданушы құрылып, сіз сәйкес хабарламаны көресіз. Экранның ортасында жаңа қолданушы үшін генерацияланған credentials-ті көресіз. Енді, олардың әрқайсына өтіп көрейік. Біріншісі – қолданушының логині. Екіншісі мен үшіншісі – AWS бағдарламасына қолжетімділігіне керек Access key ID мен Secret access key. Бағдарлама қолжетімділігі деген – AWS CLI немесе AWS SDK сервистерін қолдану. Төртіншісі – құпиясөз. Құпиясөз AWS Management Console-ге тіркелу үшін керек. Бұл ақпараттың тек осы парақшада ғана берілетініне назар аударыңыз! Сондықтан егер бұл сіздің қолданушыңыз болса, онда сіздің Secret access key, Access key ID-ді және логин мен құпиясөзді қауіпсіз жерде сақтауға кеңес беріледі. Егер сіз қолданушыны қызметкеріңіз үшін құрып жатсаңыз, онда бұл деректерді қызметкеріңіздің почтасына жіберу үшін send email функционалын қолдануға кеңес береміз. Барлық керекті ақпарат сақталған соң, біз экранның төменгі жағындағы close батырмасын басып, келесі парақшаға өтеміз. Close батырмасын басу арқылы жаңа қолданушыны құру процесін аяқтаймыз да, тіркелген қолданушылар тізімі бар алдыңғы парақшаға қайта барамыз. Экранның жоғары жағында қолданушының сәтті тіркелгені жайлы жасылмен белгіленген хабарламаны көресіз. Қолданушылардың тізімі тұрған экранның ортасынан, сондай-ақ біздің құрған қолданушымызды да көре аласыз.

Қанеки, шағын белсенділік жасап көрейік. Ол үшін бізге Amazon S3 серивисіне өту керек. Оған өту үшін іздеу жолын пайдаланайық. Amazon S3 сервисіне өткен бойда Buckets қойындысын ашамыз. Сіз мұны мәзірдің сол жақ бөлігінен көруіңіз мүмкін. Экранның ортасынан бар Bucket-тер тізімін көре аласыз. Біздің жағдаймызда бір құрылған Bucket бар. Енді AWS Management Console-іне жаңа қолданушымыз Yelzhan-мен тіркеліп көрейік. Біз бірінші рет тіркеліп тұрғандықтан, бізге құпиясөзді ауыстырып, өзіміз ғана білетін жаңасын орнату керек болады. AWS Management Console-дің негізгі парақшасына өткенде, экранның жоғары оң жағында Yelzhan деген атаумен тіркелгенімізді көреміз. Енді Amazon S3 сервисіне өтейік. Ол үшін іздеу жолын пайдаланамыз. Amazon S3 серивисіне өткен соң, Buckets қойындысы ашылып, осы аккаунтта құрылған Amazon S3 Buckets-терін көреміз. Біздің жағдайымызда Buckets-тер көрінбейді, оған қоса Create bucket батырмасы белсенді емес. Сұрақ. Неліктен бұлай болды? Сіз қазір видеоны тоқтатып, сұраққа жауап беріп көрсеңіз болады. Жақсы. Cіздердің көпшілігіңіз дұрыс жауап берді деп ойлаймын. Жауабы – иә, біз қолданушыны тіркедік. Иә, біз қолданушыны Students тобына қостық. Бірақ қолданушыда да, топта да ешқандай құқық жоқ. Қолданушы AWS аккаунтінде белгілі бір әрекет істей алуы үшін, оның ішінде бар Buckets көре алуы үшін немесе жаңа Bucket-ті құру үшін оған құқық беру маңызды.

AWS бұлтында құқық беруге AWS IAM сервисінің келесі ресурсы – IAM Policies жауапты. Yelzhan қолданушысына сәйкес құқық беру үшін қайтадан admin қолданушысы атынан тіркеліп, AWS IAM сервисіне өтіп, мәзірдің сол жағындағы Policies қойындысын ашайық. Біздің AWS аккаунтымызда 975 Policies бар екенін көреміз. Қанеки, тағы бір белсенділік жасап көрейік. Видеоны тоқтатып, жауап беріңіз. Неліктен бізде Policies-тің саны тым көп? Жақсы. Дұрыс жауабы – бұлардың көбі қолмен құрылған жоқ. Бұл – managed policy. Лекциядан білетініміздей, managed policy – AWS арқылы басқарылатын policy және сол арқылы жаңартылады, толықтырылады, құралады. Бұлтта белілі бір опцияның болсын құрылу процесін жылдамдату үшін осы policy-ді қолданамыз. Қажет болған жағдайда, өздеріңіздің custom policy-іңізді құра аласыздар. Ол үшін жоғарыдағы оң жақта create policy батырмасын бассаңыз болады. Біздің демо-сессия аясында custom policy құрмай, AWS ұсынатын policy-ді пайдаланамыз. Енді, мына policy-лер тізімін фильтрден өткізіп, тек Amazon S3-пен байланысты policy-лерді қалдырайық. Оқыту мақсатында көрінген тізімде AmazonS3FullAccess policy-ін таңдаймыз. Осы жерде біз бұлтта кез келген Identity үшін, ол Role, қолданушы немесе топ болсын, least privileged access-ті ұстану керекпіз, яғни тек керек құқықты ғана беретінімізді айта кету керек. Ары қарай жоғарыдағы оң жақтан Actions-ке кіріп, ашылмалы мәзірден Attach-ты таңдаймыз. Бұл батырманы басқан бойда барлық identity тізімі бар парақшаға өтеміз. Енді, тізімді фильтрден өткізіп, тек User groups-ті ғана қалдырайық. Фильтрден өткен тізімнен жаңа ғана өзіміз ашқан Students тобын таңдаймыз. Әрі қарай экранның төменгі оң жақ бөлігіндегі attach policy батырмасын басамыз. Бізді қайтадан Policies қойындысына лақтырады. Экранның жоғары жағынан біздің бір entity-ге AmazonS3FullAccess Policy-ді сәтті байланыстырғанымыз жайлы хабарландыруды көруге болады. Ал енді Students тобы жақтан қандай өзгерістер болғанын көрейік. Ол үшін бізге мәзірдің сол жағындағы User groups қойындысына өтіп, students тобын ашу керек. Students тобының парақшасында біз осы топтағы қолданушылардың тізімін көре аламыз, сондай-ақ Permissions қойындысынан осы топқа қосылған Policies-ты көре аламыз. Біздің жағдайымызда біз AmazonS3FullAccess-ті көріп тұрмыз. Енді қайтадан yelzhan қолданушысы арқылы тіркелейік. Экранның жоғары оң жағынан мұны жасап қойғанымызды көре аласыздар. Ары қарай Amazon S3 сервисін ашып, Buckets қойындысынан, бұл қолданушыда AWS аккаунтындағы барлық Buckets-тің көрініп тұрғанын көре аламыз. Оған қоса бізде create bucket батырмасы белсенді болды. Осылайша, біз оларға керекті құқықты бердік, ал біздің жағдайымызда Students тобы арқылы yelzhan қолданушысына бірден қолданылды.

Бүгінгі Демо-сессиямыздың соңғы бөлігі AWS IAM сервисінің соңғы ресурс түрі – IAM Role-ге арналады. Бар Roles-терді көру үшін мәзірдің сол жағындағы Roles қойындысына басыңыз. Қанеки, сіздермен жаңа Role құрып көрейік. Ол үшін экранның жоғары бөлігінің оң жағындағы Create role батырмасын басыңыз. Role құру үшін бізге экранның сол жағында көріп тұрған баптаудың 3 парақшасынан өту керек. Бірінші парақшада бізге trusted entity-ді, яғни, бұл Role кімге, не үшін құрылатынын анықтау керек. Ең танымал екі нұсқа бар. Бұл: AWS сервис, яғни біз AWS сервисі үшін ол басқа AWS сервистерді қолдана алатындай Role құрамыз. Екіншісі: біз басқа AWS аккаунт үшін Role құрамыз. Бұл өзге AWS аккаунттарының қолданушылары осы аккаунтта Role-ді қолданып, аталған аккаунттағы сервистер мен ресурстарға қолжетімділік алу үшін құрылған. Демо аясында AWS сервисіне Role құрамыз. Осы пунктті белгілеген бойда төменде таңдауға болатын сервистер тізімі шығады. Ең танымал нұсқалар: Amazon EC2 және AWS Lambda. Қанеки, AWS Lambda-ны таңдап, келесі парақшаға өту үшін next батырмасын басайық. Role құру баптауларының екінші парақшасында бізге осы Role-ге қосатын policy-ларды белгілеп шығу керек. Демо аясында біз Role-імізге AWSLambdaBasicExecutionRole деп аталатын келесі policy-ді қосамыз. Оны тез табу үшін, фильтр жолына Lambda және Basic деп енгізуіміз керек. Осы policy-ді таңдаған соң баптаулардың келесі парақшасына өту үшін экранның төменгі бөлігінің оң жағындағы next батырмасын басамыз. Баптаулардың үшінші парақшасында бізге болашақ Role-дің атауын енгізу міндеттеледі. Ары қарай қажет болған жағдайда сипаттамасын толтырсаңыз болады. Егер парақшаны төменірек айналдырсақ, trusted entity-ді сипаттайтын генерацияланған JSON-ды көреміз. Бұл trusted entity-ді бірінші қадамда енгізгенбіз. Ары қарай екінші кезеңде таңдаған, яғни осы Role-ге байланған барлық permissions көрсетіледі. Егер бұл парақшаны сәл төменге айналдырсақ, бұл Role-ге тегтер қоса алатынымызды көреміз. Демо аясында бұған толығырақ тоқталмай, Create role батырмасын басып, ары қарай жалғастырамыз. Create role батырмасын басқан соң бізді осы AWS аккаунтындағы барлық Role-дер тізімі бар парақшаға жібереді. Егер сіз Role-іңіздің атын енгізіп бастасаңыз, ол тез сортталып, бізге құрылған Role-ді көрсетеді. Сондай-ақ, экранның жоғары жағында жаңа Role-дің сәтті құрылғаны жайлы хабарламаны көре аласыздар.

Осымен біз бүгінгі Демо-сессиямызды аяқтаймыз. Біз бүгін AWS IAM сервисі мен оның компоненттерін толығырақ қарастырдық. Бұл видео сіздерге пайдалы болды деген үміттемін. Келесі сабақта кездескенше!