Қайырлы күн, құрметті студенттер! Сізді зертханалық жұмысты талдаудың кезекті сессиясында көргеніме қуаныштымын. Бұл зертханалық жұмыс AWS IAM сервисімен тереңірек танысуға арналған. Бастайық. Алдымен зертханалық жұмыстың негізгі парақшасын ашу керек. Ол үшін AWS Academy платформасын пайдаланып, осы платформаға кіріп, содан кейін қажетті курсты таңдап, төртінші модульді ашу керек, төртінші модульдің белсенділіктерінде Lab 1: Introduction to AWS IAM сілтемесі болады. Осы сілтемені басқаннан кейін сіз зертханалық жұмыстың негізгі парақшасына өтесіз. Мұнда құмсалғышты іске қосу үшін және сіздің сессияңыз үшін арнайы AWS аккаунт құрылу үшін, мәзірдегі «Start Lab» батырмасын басу керек. Зертханалық жұмысты сәтті бастағаннан кейін AWS Management Console-ге өту үшін AWS батырмасын басу керек.

Сілтемеге өткеннен кейін, сіз AWS Management Console-дің негізгі парақшасына келесіз. Назар аударыңыз, жоғарғы оң жақта сіз генерацияланған пайдаланушы арқылы авторизацияланғансыз, сонымен қатар сіз үшін бірегей AWS Account ID арнайы жасалған.

Әрі қарай, жоғарыдағы AWS сервистерінің іздеу жолағында IAM деп жазуды бастау керек. Бұл сервис тізімде бірінші болып шығады. Cоған көшейік. AWS IAM сервисінің негізгі парақшасына кіргеннен кейін, сол жақтағы навигациялық мәзірде осы AWS аккаунтта бар пайдаланушылардың тізімін көрсету үшін «Users» қойындысын басу керек. Зертханалық жұмыс аясында алдын-ала құрылған үш пайдаланушы бар – User-1, User-2 және User-3. User-1 пайдаланушысы туралы кейбір мәліметтерді көру үшін, оны ашайық. Егер сіз Permissions қойындысын ашсаңыз, онда бұл пайдаланушының оған байланған Policy жоқ екенін көруге болады. Егер мұны істеу керек болса, Add Permissions батырмасын пайдалануға болады. Келесі қойынды Groups деп аталады. Бұл қойындыда сол пайдаланушы кіретін барлық топтар көрсетіледі. Қазіргі уақытта бұл пайдаланушы топтардың ешқайсысына жатпайтынын көреміз. Келесі қойынды – Security Credentials. Бұл парақшада сіз осы пайдаланушының барлық Credentials-тарын таба аласыз. Бұл қойындыда Console Password - Enabled режимінде екенін ескеру қажет. Бұл пайдаланушының (IAM-User) AWS Management Console-ге кіру мүмкіндігі бар екенін көрсетеді.

Біз үшін қандай пайдаланушылар құрылғанын егжей-тегжейлі қарастырдық. Сондай-ақ, қалған екі пайдаланушы туралы мәліметтерді ашып, оның сәйкес келетініне көз жеткізуге болады. Әрі қарай, сол жақ навигациялық мәзірде осы AWS аккаунттағы бар топтардың тізімін ашу үшін User Groups қойындысын басу керек. Бұл AWS аккаунтта зертханалық жұмыс аясында үш топ құрылған: EC2-Admin, EC2-Support және S3-Support. EC2-Support тобын ашып, оның мәліметтерін көрейік. Ашылған парақшада Permissions қойындысына өтсеңіз, бұл топтың AmazonEC2ReadOnlyAccess деп аталатын тек қана бір тіркелген Policy бар екенін көреміз. Мұнда мен бұл Policy - AWS Managed типі бойынша құрылғанына назар аударғым келеді, яғни AWS өзі осы Policy-дің құруымен, жаңартуымен, сондай-ақ сүйемелдеумен айналысады. Бізге қолжетімді опцияларды көру үшін осы Policy-дің жанындағы plus белгішесін басыңыз. Бізге жалпы actions-тар, мысалы, "describe" және "list" сияқты операцияларға қол жетімді екенін көреміз, яғни бұл Policy-да AWS аясында ресурстарды өзгерту мүмкіндігі жоқ, оны тек оқу режимінде көруге болады. Сервистер туралы айтатын болсақ, бұл EC2, Elastic Load Balancing, CloudWatch және Autoscaling. Енді бізде келесі топ. Сол жақтағы навигация мәзірінде "User Groups" қойындысына басыңыз және ашылған топтар тізімінде S3-Support тобына өтіңіз. Мұнда біз Permissions қойындысын ашсақ, бұл топқа тіркелген AmazonS3ReadOnlyAccess деп аталатын Policy бар екенін көреміз. Ол, сондай-ақ, AWS Managed Policy болып табылады. Егер plus батырмасын бассақ, онда біз осы Policy-дің мазмұнын көреміз. Ол бізге S3 сервисі аясында get, list операцияларына қол жеткізуге мүмкіндік береді, яғни бұл Policy да read only болып табылады. Мұны тағы бір рет жасағаннан кейін, біз сол жақ навигация мәзіріндегі User Groups қойындысы арқылы бар топтардың тізімін ашамыз және EC2-Admin үшінші тобына өтеміз. Бұл топта Permissions қойындысын ашу арқылы біз бір тіркелген Policy – EC2-Admin-Policy бар екенін көреміз. Түрі бойынша, бұл Customer Inline екенін көруге болады, бұл осы Policy осы топ ішінде жеке құрылғанын көрсетеді. Plus батырмасын басу арқылы біз осы Policy-дің мазмұнын көреміз. Біз EC2 сервисі үшін describe-тен басталатын барлық операцияларға, actions-терге рұқсат берілетінін, сондай-ақ start instance және stop instance actions-теріне қосымша рұқсат берілетінін көреміз. Осылайша, біз зертханалық жұмыс аясында арнайы құрылған IAM топтарымен егжей-тегжейлі таныстық. Енді біздің IAM пайдаланушыларымызды зертханалық жұмыс тапсырмасына сәйкес тиісті топтарға қосу қажет. Ол үшін сол жақ навигациялық мәзірден User Groups қойындысына өтіп, S3-Support тобын ашамыз.

S3-Support тобының парақшасында Users қойындысына өтіп, Add Users батырмасын басыңыз. Бұл AWS аккаунтында бар пайдаланушылардың тізімі ашылады, содан кейін S3-Support тобы үшін User-1 тармағын таңдап, Add Users батырмасын басыңыз. Біз S3-Support тобының негізгі парақшасына бағытталамыз. Жоғары жағында пайдаланушылар осы топқа сәтті қосылғаны туралы жасыл түсті хабарлама пайда болады. Егер сіз “Users” қойындысын қарасаңыз, S3-Support тобына жататын пайдаланушылар тізімінде жаңадан қосылған User-1 пайдаланушысын да көреміз. Енді келесі топтармен осы әрекеттерді жасаймыз, сондықтан сол жақ навигация мәзіріндегі "User Groups" қойындысын тағы бір рет басып, EC2-Support тобына өту керек. Әрі қарай, "Users" қойындысында "Add Users" батырмасын басып, келесі "User-2" пайдаланушысын таңдап, "Add Users" батырмасын басамыз. Содан кейін біз EC2-Support парақшасына өтіп, пайдаланушының қосылғаны туралы ұқсас хабарламаны көреміз.

Әрі қарай жүрейік. Бізде үшінші топ қалды. Сол жақ навигациялық мәзірде бар топтардың тізімін көру үшін "User Groups" қойындысын басыңыз. Содан кейін үшінші EC2-Admin тобын, Users қойындысы арқылы "Add Users" батырмасын басыңыз. Пайдаланушылар тізімінде біз үшінші User-3 пайдаланушысын таңдап, "Add Users" батырмасын басамыз. Біз EC2-Admin тобының негізгі парақшасына өтіп, осы әрекетті сәтті орындағанымыз туралы тиісті хабарламаны көреміз, ал "Users" қойындысында біз User-3 пайдаланушысын көреміз. Егер сол жақ навигация мәзіріндегі User Groups қойындысын тағы бір рет бассақ, топтар тізімі ашылады және осы тізімде тиісті IAM топтарындағы пайдаланушылар санын көрсететін арнайы "Users" бағаны бар. Біз қазір әр топта бір пайдаланушы бар екенін көреміз. Егер сіз біз жасаған барлық әрекеттерді орындаған болсаңыз, соңында сізде осындай көрініс болуы керек.

Осымен пайдаланушыларды топтарға байланыстыру тапсырмасын аяқтадық. Келесі бөлімге өтеміз, атап айтқанда сол жақ навигация мәзірінде Dashboard қойындысына басайық. Парақшаның оң жағында сіз "Sign in URL for IAM users" сілтемесін көресіз, оны көшіру керек және сіз бұл сілтемені қызметкерлеріңізге тарата аласыз және олар осы сілтемені қолдана отырып, сіздің AWS аккаунтыңызда IAM пайдаланушылары ретінде кіре алады. Біз осы AWS аккаунтта біз үшін құрылған пайдаланушылардың атынан кіріп, олардың қандай сервистерге қол жеткізе алатынын немесе қол жеткізе алмайтынын көрейік.

Бұл сілтемені сізге Инкогнито режимінде ашуға кеңес беремін. Бұл парақшаны ашқаннан кейін ID аккаунтты енгізу терезесі пайда болады. Ол жазылып тұрады, өйткені ол осы сілтеменің ішінде бар. Пайдаланушының логині мен паролін енгізу жеткілікті. Пайдаланушының логині – user-1. Парольді AWS Academy-де зертханалық жұмыстың тапсырмасы бар парақшадан қарауға болады. Авторизациядан кейін оң жақ жоғарғы жағында біз сол AWS account ID, бірақ user-1 пайдаланушысы арқылы отырғанымызды көруге болады. Берілген құқықтар сол пайдаланушы үшін жұмыс істегенін білу үшін S3 қызметіне көшейік. Көріп отырғанымыздай, осы AWS аккаунтта бар бакеттер тізімі сәтті көрсетілді. Егер біз осы жалғыз бакетке бассақ, сол бакетте қандай нысандар сақталып жүктелгенін көруге болады. Осы зертханалық жұмыстың бір бөлігі ретінде бұл бакетке ешқандай нысандар жүктелмегендіктен, біз мұнда ештеңе көрмейміз.

Енді келесі бір әрекет орындайық: user-1 үшін біз EC2 сервисіне қол жеткізе алмайтынымызды біле отырып, EC2 сервисін ашамыз. Біз EC2 сервисіне кіргеннен кейін, сол жақ навигация мәзірінде Instances қойындысын басыңыз, сонда осы аймақтағы және осы AWS аккаунттағы барлық инстанстар көрсетіледі. Сіз "You are not authorized to perform this operation" деген хабарлама көресіз, бұл бізде инстанстар тізімін көрсету үшін жеткілікті құқықтарымыз жоқ дегенді білдіреді. Мұнда айта кету керек, тіпті ресурстар тізімін көрсетудің өзі бөлек қол жетімділікті қажет етеді. Осылайша, AWS бұлтының ішіндегі қолжетімділіктерді мүмкіндігінше егжей-тегжейлі реттеуге болады.

Біз user-1 пайдаланушысымен аяқтадық, жоғарғы оң жақтағы аккаунт ID-ге барып, басқа пайдаланушы арқылы кіру үшін ашылмалы мәзірде "sign out" батырмасын басыңыз. Енді user-2 пайдаланушысы арқылы біздің AWS аккаунтымызға кірейік. Ол үшін біз алдында көшіріп алған сілтемені қолданамыз. User name-ге user-2 деп енгіземіз, сондай-ақ AWS Academy-дегі зертханалық жұмыстың тапсырмасы берілген парақшасынан парольді енгізу қажет. Авторизациядан кейін жоғарғы оң жақта user-2 пайдаланушысы арқылы авторизацияланғаныңызға назар аударыңыз. Егер бәрі дұрыс болса, біз EC2 сервисіне өтеміз. Естеріңізге сала кетейін, user-2 пайдаланушысы үшін біз EC2 сервисіне оқу режимінде ғана жұмыс істеу құқығын бердік. Осылайша, бізде North Virginia аймағында бар инстанстардың тізімін көрсетуге құқығымыз бар. Мұны тексеру үшін Instances деп аталатын сол жақ навигация мәзіріндегі қойындыға өтіңіз. Ол аймақтағы инстанстардың тізімін көрсетуі керек. Егер инстанстардың тізімі көрсетілмесе, ол бос болса, онда жоғарғы оң жақта аймақ ретінде North Virginia таңдалғанын тексеріңіз. Егер сізде басқа аймақ таңдалған болса, оның атауын басып, аймақтар тізімінің ішінде North Virginia аймағын немесе us-east-1 жүйелік атауын таңдау керек. Мұны жасағаннан кейін сіз North Virginia аймағында бар инстанстардың тізімін көрсетесіз және келесі екі инстансты көресіз. User-2 пайдаланушы үшін тек оқу режимінде құқық берілгені есімізде. Дегенмен, LabHost инстансымызды тоқтатып көрейік. Тізімнен біздің LabHost инстансын таңдаймыз, жоғарғы оң жақта Instance state батырмасын басып, ашылмалы тізімде Stop Instance әрекетін таңдау керек. Бұл инстансты шынымен тоқтатқымыз келетін-келмейтінін растауды сұрайтын хабарлама пайда болады. Instance ID және жақша ішінде осы инстанстың аты көрсетіледі, осы инстанстың тоқтатуын растау үшін Stop батырмасын басыңыз. Басқаннан кейін, бұл пайдаланушының осындай ID-і бар инстансты тоқтатуға құқығы жоқ екендігі туралы қызыл түсті хабарлама пайда болады. Бұл хабарламаны жабайық.

Енді S3 сервисіне өтейік. Біз user-2 пайдаланушысы үшін S3 сервисіне құқық берілмегенін білеміз. Осылайша, егер біз сол жақтағы навигациялық мәзірден Buckets қойындысына өтсек, бакеттер тізімі көрсетіледі, бірақ бұл тізім бос болады. Бұл Implicit Deny-дің жұмыс істегенін көрсетеді, яғни әдепкі бойынша, біз AWS ресурстарына кіруге тыйым саламыз. Осымен біз user-2 пайдаланушысымен аяқтаймыз. Жоғарғы оң жақта Account ID таңдап, ашылмалы мәзірде шығу үшін Sign out батырмасын басамыз.

Соңғы тапсырма – User-3 пайдаланушысы арқылы AWS аккаунтта не істей алатынымызды көру. Естеріңізде болса, User-3 пайдаланушысының басқа пайдаланушыларға қарағанда айырмашылығы, read only қолжетімділігінен басқа, бұл пайдаланушыға инстанс EC2-ді тоқтатуға және қосуға құқығы берілген. Осы пайдаланушыны арқылы кіріңіз. User-3 логині, парольді зертханалық жұмыстың тапсырмасы берілген AWS Academy парақшасынан таба аласыз.

Авторизациядан кейін жоғарғы оң жақта User-3 пайдаланушысы арқылы отырғанымызды міндетті түрде тексеріңіз. Әрі қарай, EC2 сервисіне өтуіміз керек, сондықтан біз жоғарғы AWS сервистерін іздеу жолағына EC2 деп енгіземіз. Біз EC2 сервисіне өткеннен кейін, сол жақ навигация мәзірінде Instances қойындысын басыңыз. North Virginia аймағында екеніңізге көз жеткізіңіз. Бәрі дұрыс болса, келесі екі инстанс көрсетілуі керек. Labhost инстансын таңдап, осы инстансты тоқтатып көрейік. Ол үшін instance state батырмасын басып, ашылмалы әрекеттер тізімінен stop instance таңдаңыз. Растау терезесі пайда болады, шынымен біз осындай инстанс ID-і бар LabHost инстансын тоқтатқымыз келеді ме. Иә, біз оны тоқтатқымыз келеді, сондықтан Stop батырмасын басамыз. Келесі парақшада біз осы инстансты тоқтату үшін белгілі бір қадамдар жасағанымыз туралы жасыл түсті хабарлама шыққанын көресіз. Инстанстар тізімінде instance state, яғни бұл инстанстың күйі "stopping" режимінде, тоқтату процесінде тұрғанын көруге болады. Біраз уақыттан кейін, refresh батырмасын басу арқылы, яғни инстанстар тізімі жаңартылғаннан кейін, біз оның статусы "stopped" болып өзгергенін көреміз, яғни ол толығымен тоқтатылды.

Осылайша, біз бұл тапсырманы зертханалық жұмыстың бір бөлігі ретінде аяқтадық. Инкогнито режимінде ашылған бұл терезені жабуға болады. Әрі қарай, бізде AWS батырмасын басу арқылы зертханалық жұмыстың тапсырмасы берілген парақшадан AWS Management Console парақшасына өткен кезде шартты root пайдаланушысы бар парақша бар. Бұл дәл сол парақша және осы аккаунттан сәтті және дұрыс шығайық. Мұны істеу үшін жоғарғы оң жақта Account ID басып, ашылмалы әрекеттер тізімінде төменгі жағында "sign out" батырмасын басу керек. Осындай хабарламаны көресіз, яғни бәрі жақсы, біз бұл парақшаны жаба аламыз.

Сондай-ақ, болашақта келесі зертханалық жұмыстарды ашуда проблемалар туындамауы үшін зертханалық жұмысты дұрыс аяқтауды ұмытпаңыз. Ол үшін AWS Academy парақшасында және әсіресе зертханалық жұмыс парақшасында жоғарғы оң жақтағы негізгі мәзірде "end lab" батырмасын басу керек. Бұл зертханалық жұмысты шынымен тоқтатқымыз келетінін растайтын қалқымалы терезені ашады. Иә, біз тоқтатқымыз келеді, сондықтан "Yes" батырмасын басамыз. Осыдан кейін тағы бір қалқымалы терезе пайда болады, онда "you may close this message box now" деген хабар болады. Бұл сіздің AWS аккаунт үшін арнайы жасалған барлық ресурстарды жою процесі басталғанын көрсетеді. Енді ол фондық режимде жұмыс істейді және сіз бұл терезені қауіпсіз жаба аласыз. Сондай-ақ, сіз AWS Academy парақшасын жауып, зертханалық жұмысты аяқтай аласыз. Құттықтаймің, біз сіздермен бірге AWS IAM сервисіне арналған зертханалық жұмысты аяқтадық. Осымен сіздермен қоштасамын, келесі белсенділіктерімізде кездескенше!