Computatio: Journal of Computer Science and Information Systems, 3/1 (2019), 1-10

TEKNIK IDENTITY AND ACCESS MANAGEMENT PADA LAYANAN AMAZON WEB SERVICES

Dhimas Dirgantara[1], Is Mardianto[2]
[1,2] Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Trisakti
Jln. Letjen S. Parman No. 1, Jakarta, 11440, Indonesia
E-mail: [1]dhimas064001400009@std.trisakti.ac.id, [2]mardianto@trisakti.ac.id

Abstrak

Pada era ini, teknologi tradisional seperti memiliki server dan berbagai macam hardware telah ditinggalkan oleh perusahaan besar, yang beralih pada teknologi cloud computing. Teknologi ini memudahkan perusahaan dalam menjalankan bisnisnya. Dari banyaknya penyedia layanan cloud computing, Amazon Web Service (AWS) adalah salah satu penyedia layanan pertama dan yang terbesar. Masalah-masalah yang terjadi dalam penggunaan teknologi cloud computing adalah pemberian hak akses dalam melakukan manajemen data. AWS memiliki suatu layanan untuk mengatur kendali akses pada setiap layanan yaitu Identity and Access Management (IAM). Layanan ini berupaya mencegah aktivitas yang mengarah pada pelanggaran keamanan. Hasil yang didapatkan berupa group yang dapat mengakses layanan AWS sesuai dengan role yang diberikan.

Kata kunci*—Cloud Computing, Amazon Web Service, Access Control, IAM, EC2*

Abstract

In this era, traditional technologies such as having servers and various kinds of hardware have been abandoned by large companies, which are turning to cloud computing technology. This technology makes it easier for companies to run their business. Of the many cloud computing service providers, Amazon Web Service (AWS) is one of the first and biggest service providers. Problems that occur in the use of cloud computing technology is the provision of access rights in data management. AWS has a service to manage access control for each service, namely Identity and Access Management (IAM). This service seeks to prevent activities that lead to security breaches. The results obtained are in the form of groups that can access AWS services according to the role given.

Keywords—*Cloud Computing, Amazon Web Service, Access Control, IAM, EC2*

1. PENDAHULUAN

Perkembangan teknologi komputer terbaru saat ini adalah cloud computing. Para pengembang aplikasi berbasis web maupun mobile kini tidak perlu pusing memikirkan untuk memiliki server sendiri. Teknologi cloud computing dapat menjalankan sebuah virtual server dengan kapasitas dan kecepatan kerja yang sangat tinggi. Cloud computing adalah sebuah kombinasi pemanfaatan teknologi komputer dan internet.

Sebagian masalah keamanan yang muncul di cloud computing adalah pengelolaan akses informasi yang ada pada teknologi cloud. Perusahaan harus menyediakan akses informasi untuk user, baik di dalam maupun di luar organisasi, tanpa membahayakan keamanan atau mengekspos informasi sensitif. Tujuan dari penelitian ini adalah untuk mengetahui fungsi role

dalam setiap group yang berbeda-beda. Resource apa saja yang didapatkan dalam sebuah role, dampak dari mengakses layanan yang tidak sesuai dengan role yang diberikan dan mengetahui model akses yang diterapkan pada layanan Identity and Access Management (IAM).

2. METODE PENELITIAN

2.1 Cloud Computing

Sejarah Cloud Computing berawal dari teknologi pendahulunya yaitu client-server dan komputasi terdistribusi peer-to-peer [1]. Menurut National Institute of Standards and Technology (NIST) Cloud computing adalah bentuk layanan yang memungkinkan pengguna melakukan akses jaringan dari manapun dengan cepat dan mudah [2].

2.2 *Akses Kontrol*

Akses Kontrol adalah mekanisme yang membatasi akses ke sumber daya. Mekanisme ini adalah sebuah tindakan pencegahan terhadap penggunaan sumber daya yang tidak sah dengan mencegah intrusi pengguna yang tidak sah atau kelalaian dari pengguna yang sah [3].

Sistem akses kontrol memiliki sebuah kriteria yaitu peran, grup, lokasi, waktu dan tipe transaksi [4]. Akses kontrol juga memiliki banyak model mekanisme yang mengatur sebuah subjek untuk mengakses sebuah objek, ada tiga tipe utama model akses kontrol yaitu:

- Discretionary
- Mandatory
- Nondiscretionary (role-based)

Discretionary adalah model akses kontrol yang memungkinkan pengguna memberikan izin kepada pengguna lain untuk mengakses data. Discretionary membatasi hak akses pada objek berdasarkan identitas subjek. Identitas ini dapat berupa identitas pengguna atau identitas grup. Grup adalah entitas yang didefinisikan oleh pembuat, sehingga dapat mengakses atau memodifikasi objek tertentu [5].

Mandatory didasarkan pada label keamanan yang melekat pada subjek dan objek. Label pada objek disebut klasifikasi keamanan, sedangkan label pada subjek disebut izin keamanan [6]. Klasifikasi tingkat keamanan berdasarkan sistem militer, kerahasiaan adalah hal yang paling penting dari data yang Unclassified sampai top secret. Subjek dapat mengakses objek yang mempunyai level sama atau lebih rendah [4].

Nondiscretionary atau biasa disebut roled-based acces control adalah kebijakan berdasarkan hak dan izin yang diberikan kepada grup atau peran, bukan kepada pengguna individu. Dalam model ini administrator akan memberikan izin kepada peran atau grup yang dibuat [7].

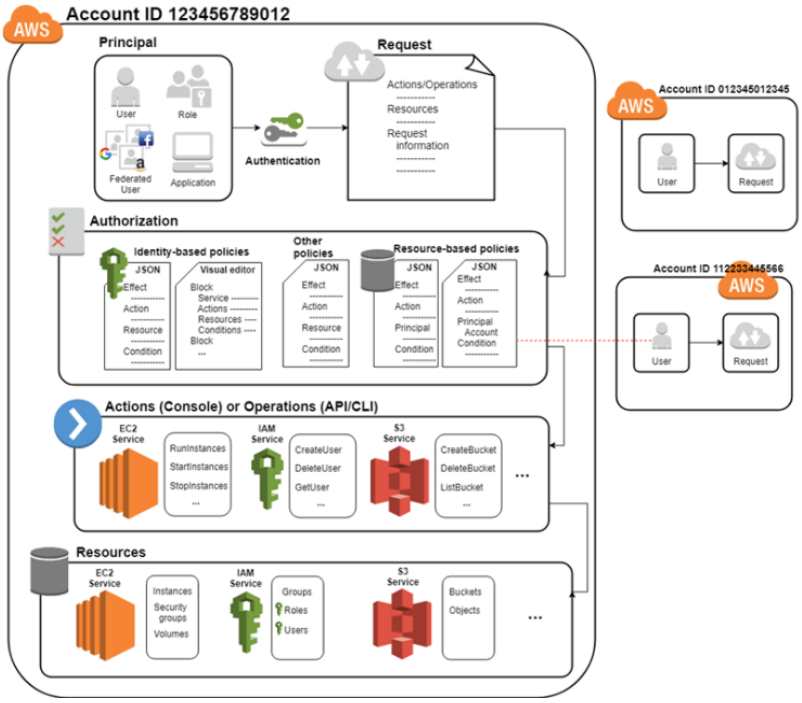
2.3 *Identity and Access Management (IAM)*

AWS Identity and Access Management (IAM) adalah sebuah layanan yang memungkinkan user untuk mengelola akses ke layanan dan sumber daya AWS. Dengan menggunakan IAM, user dapat membuat dan mengelola user lain dan membuat grup user AWS. User juga dapat memberikan izin untuk mengizinkan dan menolak akses mereka ke sumber daya AWS [8].

Berikut ini adalah manfaat dari menggunakan IAM, yaitu:

- Enhanced Security. IAM memungkinkan user admin memberikan kredensial keamanan unik kepada pengguna dan grup, untuk menentukan cara mengakses sumber daya AWS.
- Granular control. IAM memberikan perincian untuk mengontrol akses pengguna ke sumber daya AWS. Seperti, mengakhiri instance EC2 atau membaca konten bucket Amazon S3.
- Temporary Credentials. Memungkinkan user admin menentukan izin, kemudian membiarkan pengguna terautentikasi. Seperti pada instance EC2, user mendapatkan akses sementara ke sumber daya yang admin tetapkan.
- Flexible security credential management. IAM memungkinkan untuk mengotentikasi pengguna dengan beberapa cara. Admin dapat menetapkan berbagai kredensial keamanan termasuk passwords, key pairs, dan X.509 certificates. Admin juga dapat menerapkan multi-factor authentication (MFA) pada pengguna yang mengakses Konsol Manajemen.
- Leverage external identity systems. Admin dapat memberi karyawan akses aplikasi ke Konsol Manajemen layanan AWS, menggunakan sistem identitas yang ada. AWS mendukung federasi dari sistem perusahaan seperti Microsoft Active Directory serta layanan penyedia identitas eksternal seperti Google dan Facebook.

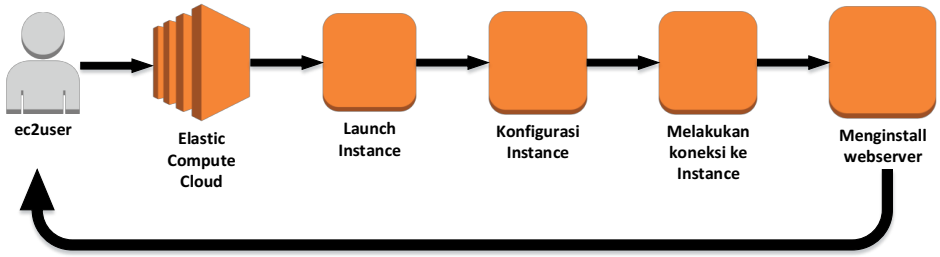
Secara umum proses user IAM mengakses layanan AWS ditunjukkan pada Gambar 1.



Gambar 1 Skema User Identity and Access Management (IAM) Mengakses Layanan [9]

2.4 Elastic Compute Cloud (EC2)

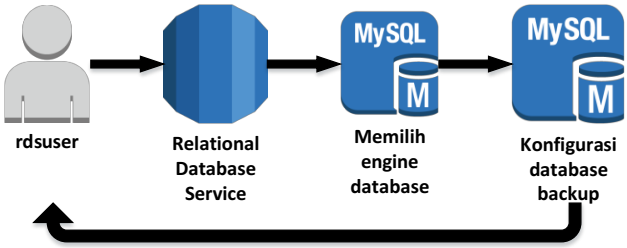
Amazon Elastic Compute Cloud (Amazon EC2) merupakan salah satu layanan AWS yang paling awal. Amazon EC2 adalah layanan yang menyediakan virtual server yang aman dan dapat dengan mudah diubah spesifikasinya. Antarmuka layanan EC2 yang sederhana memudahkan user untuk mengkonfigurasi virtual server yang digunakan. Membuat user memiliki kontrol penuh atas komputasi sumber daya. Amazon EC2 mengurangi waktu yang dibutuhkan dalam melakukan instalasi server dalam hitungan menit, memungkinkan user dengan cepat menambah maupun mengurangi kapasitas [10]. Pada Gambar 2 ditunjukkan ec2user yang telah diberikan role dalam group EC2Developer membuat sebuah instance.



Gambar 2 Skema Elastic Compute Cloud (EC2)

2.5 Amazon Relational Database Service (Amazon RDS)

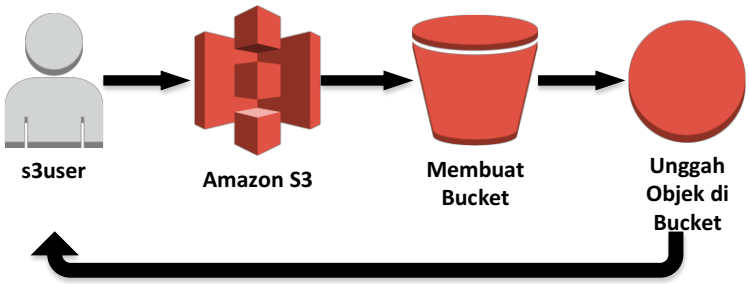
Amazon Relational Database Service (Amazon RDS) memudahkan untuk mengatur, mengoperasikan, dan menskalakan basis data relasional di cloud. Amazon RDS menyediakan kapasitas yang dapat diubah ukurannya [11]. Amazon RDS menangani tugas-tugas basis data seperti provisioning, patching, backup, recovery, failure detection, dan repair. Proses pembuatan instance menggunakan rdsuser yang telah diberi kebijakan full access layanan RDS ditunjukkan pada Gambar 3.



Gambar 3 Skema Relational Database Service (RDS)

2.6 Amazon Simple Storage Service (Amazon S3)

Layanan Simple Storage Service atau dikenal dengan S3 adalah layanan AWS dalam penyimpanan objek yang dibuat untuk menyimpan dan mengambil sejumlah data. Layanan penyimpanan dapat memuat berbagai ekstensi file, dan dapat digunakan juga untuk menjalankan sebuah web statis [12]. Proses bucket yang dibuat ditunjukkan pada Gambar 4, menggunakan s3user sebagai pemegang akses penuh layanan S3.

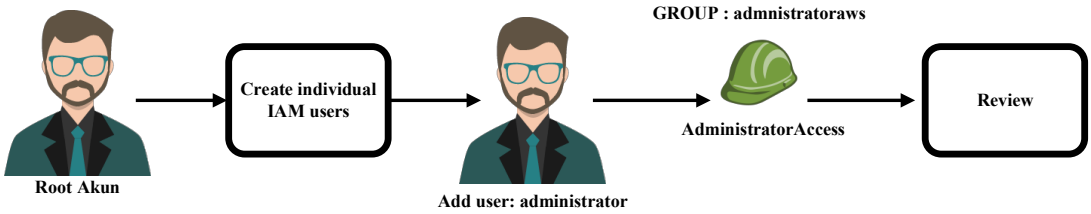


Gambar 4 Skema Simple Storage Service (S3)

Uji coba dilakukan dengan memberikan hak akses berdasarkan peran yang dilakukan pada setiap layanan. User yang dibuat dapat mengakses penuh sesuai layanan yang diberikan dan diberikan akses membaca layanan yang berhubungan. Setiap User dicoba pada layanan yang berbeda untuk melihat dampak yang terjadi sesuai dengan Role yang telah diberikan.

3. HASIL DAN PEMBAHASAN

User pertama yang dibuat diberikan hak akses penuh terhadap semua layanan yang ada di AWS kecuali layanan pembayaran. User administrator ini untuk menghindari penggunaan root akun karena memiliki akses yang tidak terbatas pada layanan. Proses pembuatan IAM digambarkan dengan diagram pada Gambar 5.



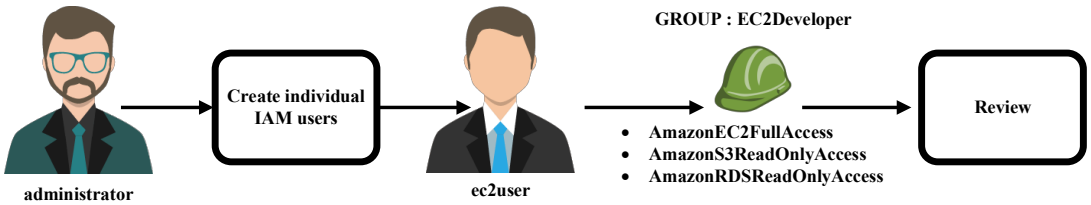
Gambar 5 Skema Pembuatan administrator

Pembuatan user akun yang memiliki hak akses penuh pada layanan AWS melalui Create individual IAM users. User administrator dibuatkan group dengan kategori level access sesuai role yang diberikan. Group administratoraws menjadi tempat kebijakan AdministratorAccess untuk mendapatkan akses penuh ke layanan dan sumber daya AWS.

Saat berperan menjadi administrator, dibuat kebijakan baru pada bagian Policy di layanan IAM untuk menambahkan fitur multi-factor authentication (MFA). Kebijakan ini tidak ada pada pilihan default dalam role yang disediakan AWS. Kebijakan baru ditambahkan dengan JSON editor seperti yang ditunjukkan pada Gambar 6.

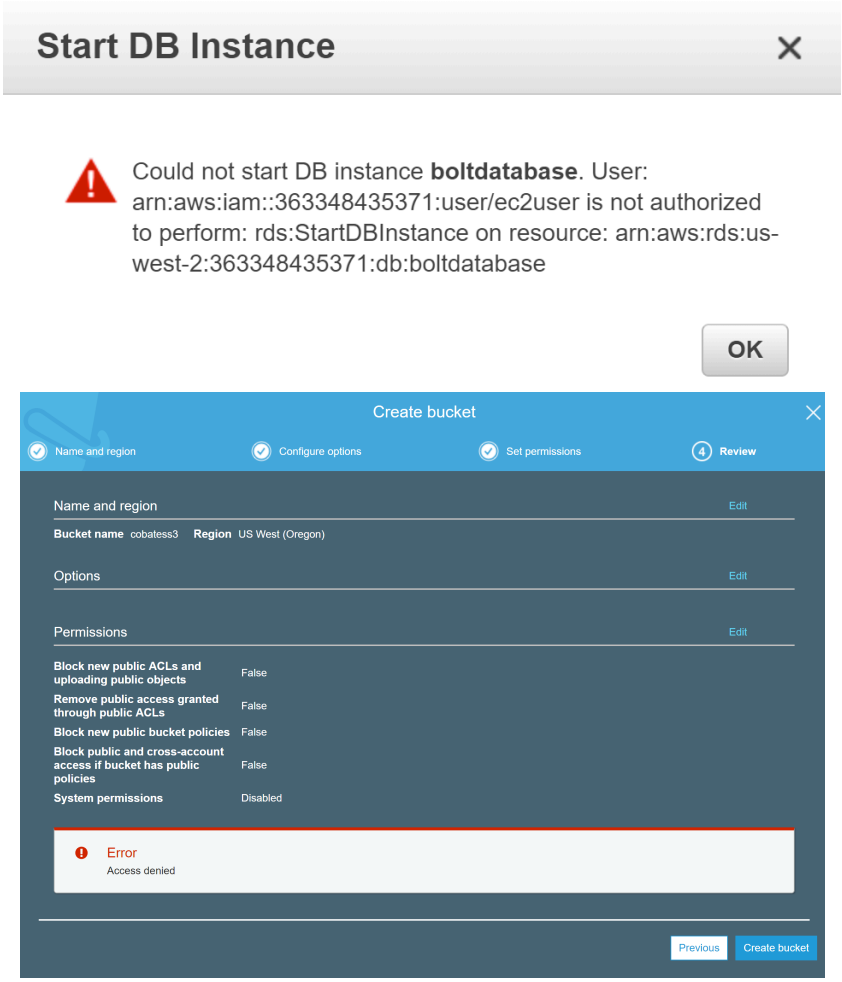
```
53          "Sid": "AllowIndividualUserToManageTheirOwnMFA",
54          "Effect": "Allow",
55          "Action": [
56              "iam:CreateVirtualMFADevice",
57              "iam:DeleteVirtualMFADevice",
58              "iam:EnableMFADevice",
59              "iam:ResyncMFADevice"
```

Gambar 6 JSON Menambahkan MFA

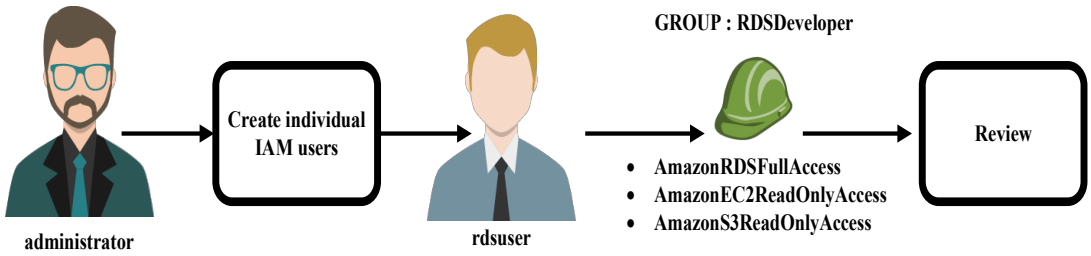


Gambar 7 Skema Pembuatan ec2user

Selain kebijakan baru, administrator membuat user baru dengan kemampuan mengakses penuh layanan EC2. Proses pembuatan ec2user digambarkan secara sederhana pada Gambar 7. User ec2user berada pada group EC2Developer yang diberikan role AmazonEC2FullAccess, AmazonS3ReadOnlyAccess, AmazonRDSReadOnlyAccess dan selfmanagedaccount. Tidak hanya dapat mengakses penuh layanan EC2, user ini dapat melihat pada layanan S3 dan RDS. Kebijakan selfmanagedaccount membuat ec2user memiliki kemampuan untuk menambahkan MFA secara mandiri melalui layanan IAM. Hasil kebijakan dapat dilihat pada Gambar 8, dengan cara menjalankan instances pada layanan RDS dan membuat bucket baru pada S3 .

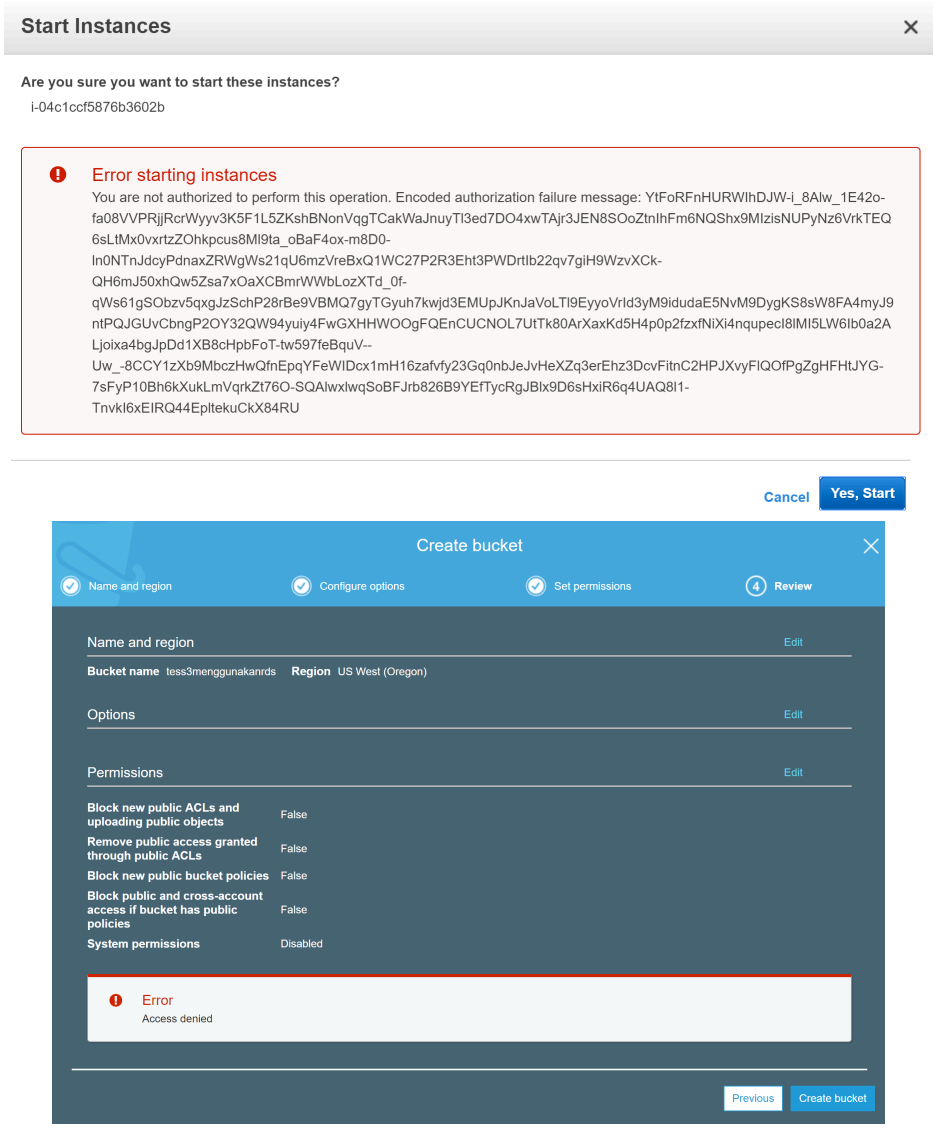


Gambar 8 Akses ec2user Ditolak Saat Menjalankan Instances RDS Dan Pembuatan Bucket S3

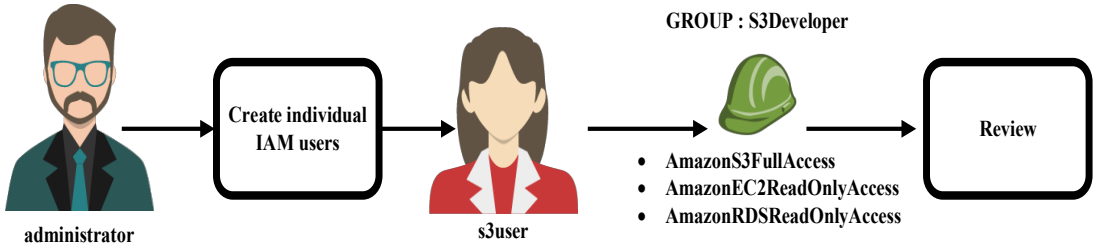


Gambar 9 Skema Pembuatan rdsuser

User rdsuser termasuk dalam group RDSDeveloper yang diberikan role AmazonRDSFullAccess, AmazonEC2ReadOnlyAccess dan AmazonS3ReadOnlyAccess seperti ditunjukkan pada Gambar 9. Dengan role tersebut user dapat mengakses penuh layanan RDS dan melihat pada layanan EC2 dan S3. Hasil kebijakan dapat dilihat pada Gambar 10, dengan cara menjalankan instances EC2 dan membuat bucket baru pada S3.

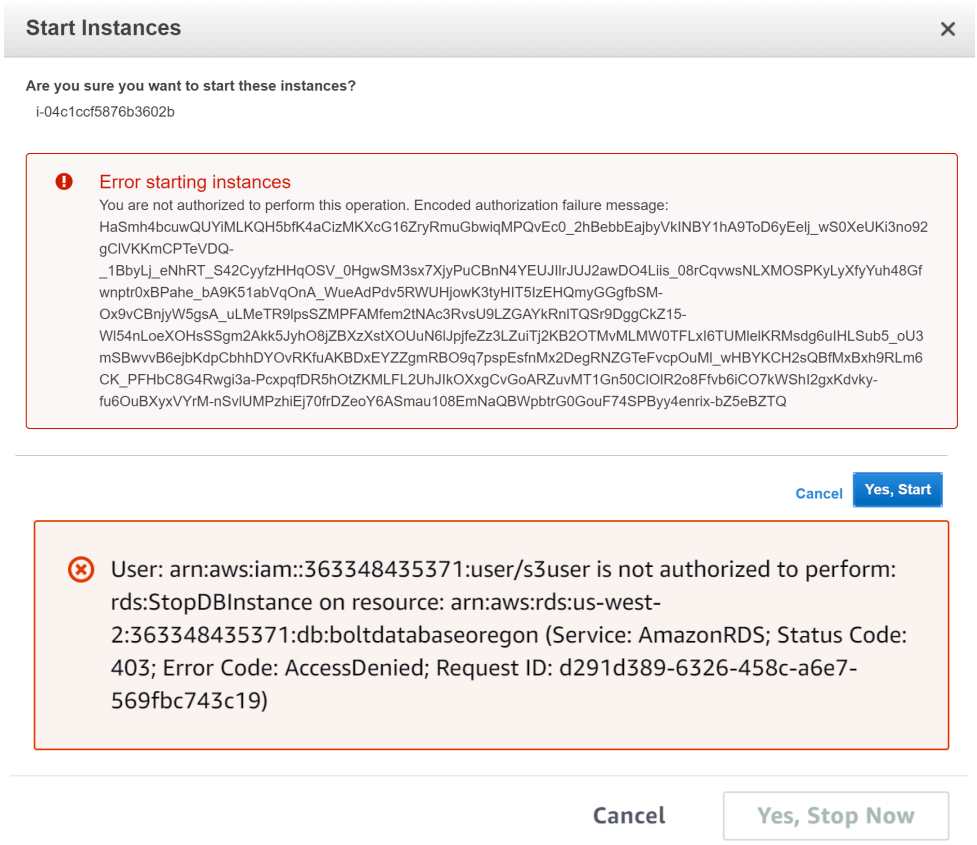


Gambar 10 Akses rdsuser Ditolak Saat Menjalankan Instances EC2 Dan Pembuatan Bucket S3



Gambar 11 Skema Pembuatan s3user

Terakhir adalah s3user yang berada dalam S3Developer. Group ini diberikan role AmazonS3FullAccess, AmazonEC2ReadOnlyAccess dan AmazonRDSReadOnlyAccess seperti pada Gambar 11. Selain dapat mengakses penuh layanan S3, s3user dapat membaca layanan EC2 dan RDS. Hasil kebijakan dapat dilihat pada Gambar 12, dengan cara menjalankan instances EC2 dan menghentikan instances RDS.



Gambar 12 Akses s3user Ditolak Saat menjalankan instances EC2 Dan menghentikan instances RDS

Tabel 1 Hasil Uji Coba Level Access User IAM berdasarkan Role yang diberikan

User	Group	Role	Resources & Level Access
administrator	administratoraws	AdministratorAccess	Semua service : Full access
ec2user	EC2Developer	AmazonEC2FullAccess	EC2 : Full access
			ELB : Full access
			CloudWatch : Full access
			IAM : Limited: Write
		AmazonRDSReadOnlyAccess	RDS : Full: List Limited: Read
		AmazonS3ReadOnlyAccess	S3 : Full: Read Limited: List
rdsuser	RDSDeveloper	AmazonRDSFullAccess	RDS : Full access
			SNS : Limited: List, Write
			IAM : Limited: Write
			CloudWatch : Limited: Read, Write

		AmazonEC2ReadOnlyAccess	EC2 : Full: List Limited: Read
		AmazonS3ReadOnlyAccess	S3 : Full: Read Limited: List
s3user	S3Developer	AmazonS3FullAccess	S3 : Full access
		AmazonEC2ReadOnlyAccess	EC2 : Full: List Limited: Read
		AmazonRDSReadOnlyAccess	RDS : Full: List Limited: Read

Berdasarkan yang penulis kerjakan didapatkan level access setiap layanan yang di gambarkan pada Tabel 1. Penulis melakukan kategorisasi dengan membuat group sesuai layanan yang dikerjakan. Dalam Tabel 1 terdapat kolom resources dan level access. Level access memiliki pengelompokkan yaitu Full dan Limited. Full memiliki makna kebijakan akses ke semua tindakan dalam klasifikasi yang ditentukan. Sedangkan Limited memiliki makna kebijakan akses ke satu atau lebih, tetapi tidak semua tindakan dalam klasifikasi level access yang ditentukan. Pada kolom ini terdapat juga keterangan klasifikasi level access yaitu List, Read dan Write. Level access List bermakna dapat melihat daftar untuk menentukan keberadaan sebuah objek. Level access Read bermakna memberikan izin untuk membaca tetapi tidak dapat mengubah konten. Terakhir level access Write untuk membuat, menghapus, atau memodifikasi sumber daya dalam layanan.

Group pertama adalah administratoraws dengan user administrator. Group administratoraws memiliki role AdministratorAccess yang dapat mengakses penuh terhadap semua layanan yang ada di AWS.

Group kedua adalah EC2Developer dengan user ec2user. Memiliki role AmazonEC2FullAccess untuk akses penuh terhadap layanan EC2. AmazonEC2FullAccess memiliki sumber daya lain seperti Elastic Load Balancing (ELB) digunakan untuk membagi trafik yang mengakses server, CloudWatch untuk melakukan monitoring dan manajemen server pada layanan EC2. Sumber daya ELB dan CloudWatch memiliki level access Full Access. Dalam role AmazonEC2FullAccess terdapat juga sumber daya IAM yang memiliki level access limited Write, hanya untuk melakukan service-linked roles. Group EC2Developer juga diberikan akses terhadap layanan RDS dan S3 dengan role AmazonRDSReadOnlyAccess dan AmazonS3ReadOnlyAccess, untuk dapat melihat objek yang ada di layanan tersebut. Pada group EC2developer diberikan kebijakan selfmanagedaccount untuk dapat menggunakan fitur MFA secara mandiri.

Group ketiga adalah RDSDeveloper dengan user rdsuser. Group RDSDeveloper memiliki role AmazonRDSFullAccess yang dapat mengakses penuh pada layanan RDS dan beberapa sumber daya lainnya. Sumber daya lain yang terdapat pada role AmazonRDSFullAccess adalah Simple Notification Service (SNS), IAM dan CloudWatch. SNS memiliki level access List untuk melihat daftar subscriptions pengguna, sedangkan level access Write untuk melakukan broadcast pesan pada pengguna. Sumber daya IAM juga terdapat pada role AmazonRDSFullAccess dengan level access limited Write. CloudWatch memiliki level access limited Read untuk mendapatkan metric statistics dan level access Write untuk membuat atau update alarm. Group RDSDeveloper diberikan role AmazonEC2ReadOnlyAcces dan AmazonS3ReadOnlyAccess untuk melihat objek pada layanan EC2 dan S3.

Group terakhir adalah S3Developer dengan user s3user yang memiliki role AmazonS3FullAccess dengan akses penuh terhadap layanan S3. Group S3Developer juga diberikan role AmazonEC2ReadOnlyAccess dan AmazonRDSReadOnlyAccess untuk melihat objek pada layanan EC2 dan RDS.

4. KESIMPULAN

Teknik IAM mengamankan sebuah perusahaan dalam pembagian akses layanan pada teknologi cloud computing. Layanan cloud computing AWS yang digunakan disesuaikan dengan kebutuhan perusahaan, dalam jurnal ini penulis membagikan hak akses untuk layanan yang paling sering digunakan yaitu layanan EC2, RDS dan juga S3. IAM sebagai layanan pemberian hak akses di teknologi cloud AWS dapat disimpulkan memiliki model akses control discretionary, karena hak akses yang diberikan berbasis identitas. Identitas disini bisa diberikan langsung pada masing-masing User atau dibuatkan Group terlebih dahulu. Penggunaan fitur MFA secara mandiri, terdapat pada layanan IAM. Tetapi AWS tidak memiliki kebijakan yang sudah jadi untuk penggunaan fitur MFA. Sebaiknya kebijakan mengaktifkan MFA dibuat menjadi salah satu pilihan yang dapat langsung digunakan seperti kebijakan lainnya. Keuntungan penggunaan teknologi IAM dapat memonitor kegiatan yang dilakukan user saat mengakses sebuah layanan, jika terjadi kesalahan penggunaan hak akses dapat langsung di investigasi.

DAFTAR PUSTAKA

[1] Michael Miller, *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online*. Indianapolis: QUE, 2008.

[2] P. M. Mell and T. Grance, “The NIST definition of cloud computing,” Gaithersburg, MD, 2011.

[3] J. Wu, Z. Lei, S. Chen, and W. Shen, “An access control model for preventing virtual machine escape attack,” *Futur. Internet*, vol. 9, no. 2, 2017.

[4] D. Kim and M. G.Solomon, *Fundamentals of Information Systems Security - 5th Edition*, 5th Editio. Canada: Jones & Bartlett Learning, 2010.

[5] P. Case and K. V Chaudhari, “A Survey on Secure Access Control Mechanism of Geospatial Data,” vol. 2, no. 2, pp. 188–194, 2014.

[6] S. Osborn, R. Sandhu, and Q. Munawer, “Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies,” vol. 2, no. 2, pp. 85–106, 2000.

[7] A. P. S. A. Ubale and S. S. Apte, “Comparison of ACL Based Security Models for securing resources for Windows operating system,” pp. 63–64, 2014.

[8] “IAM Product Details - Amazon Web Services (AWS).” [Online]. Available: https://aws.amazon.com/iam/details/. [Accessed: 20-Mar-2018].

[9] A. W. Services, “AWS Identity and Access Management User Guide.”

[10] “Amazon EC2.” [Online]. Available: https://aws.amazon.com/ec2/. [Accessed: 20-Mar-2018].

[11] “Amazon Relational Database Service (RDS) – AWS.” [Online]. Available: https://aws.amazon.com/rds/?nc2=h_m1. [Accessed: 20-Mar-2018].

[12] “Cloud Object Storage | Store & Retrieve Data Anywhere | Amazon Simple Storage Service.” [Online]. Available: https://aws.amazon.com/s3/?nc2=h_m1. [Accessed: 09-Jul-2018].