DIGITALENT

CLOUD COMPUTING ITB

Mirza Ichwanul Aziz

AWS WAF *Summary*

AWS Well Architected Framework merupakan sebuah panduan yang praktis untuk customer dan partner dari AWS untuk melihat apakah architecture sistem mereka sudah baik atau belum. AWS WAF memiliki lima pilar yaitu *operational excellency, security, reliability, performance efficiency dan cost optimization. Operational excellency* adalah kemampuan untuk mendukung pengembangan yang efektif. *Security* adalah pilar yang mencakup kemampuan untuk melindungi data, sistem dan asset. *Reliability* mencakup kemampuan sebuah *workload* untuk melakukan fungsinya dengan benar dan konsisten. *Performance efficiency* adalah kemampuan untuk menggunakan *resources* secara efisien untuk memenuhi kebutuhan sistem. *Cost optimization* adalah kemampuan sistem untuk berjalan dengan modal yang seminimal mungkin tetapi dapat men-*deliver business value* yang besar. Beberapa istilah dalam AWS WAF seperti *component, workload, architecture, milestone dan technology portofolio.* Ketika merancang *workload,* kelima pilar tadi harus dipertimbangkan dengan matang sesuai dengan *business value* yang diinginkan. Bisa saja kita membuat sistem dengan tingkat *security system* yang tinggi dengan mengorbankan *performance efficiency* atau *cost optimization*. Semua harus disesuaikan dengan kebutuhan masing-masing *customer*. Terdapat 6 prinsip desain dari AWS WAF. Pertama, kapasitas yang fleksibel sesuai dengan kebutuhan. Kedua, pengujian sistem di *production scale*. Ketiga, automasi yang ada dapat membantu berjalannya sistem. Keempat, *architecture* yang dapat dikembangkan terus menerus. Kelima, data untuk mengendalikan *architecture.* Terakhir, *improvements* yang bisa dilakukan setiap harinya.

Security – encryption & data in transit

Salah satu *design principle* dalam *security* di AWS WAF adalah, data harus di proteksi di level *transit* dan *rest*. Proteksi bisa dilakukan dengan *encryption, tokenization* dan pembagian akses control. Sebelum melakukan proteksi data, pertama harus dilakukan klasifikasi data terlebih dahulu, dan melihat mana data yang paling penting. Serta untuk menentukan tingkat proteksi data. AWS *customer* memiliki control penuh terhadap data. Hal ini didukung dengan AWS yang membuat *user* lebih mudah untuk enkripsi data, *manage keys*, *key rotation.* AWS juga merancang agar *data logging* untuk data yang penting. Ada dua tipe data, yaitu *data at rest* dan *data in transit.* Cara proteksi *data at rest* adalah dengan implementasi *multiple controls* untuk mengurangi resiko akses tidak terautorisasi. Cara proteksi ada beberapa fitur yang bisa digunakan, yaitu server-side-encryption (SSE) untuk Amazon S3, HTTPS *encryption and decryption process (SSL Termination).* Bisa juga dilakukan dengan *certificate management,* seperti dengan merotasi penyimpanan *encryption keys* dan sertifikat selama interval waktu atau dengan menggunakan AWS Certificate Manager.