Infrastruttura cloud AWS per Senonet

Versione 2.0 del 16/03/2023

Infrastruttura cloud AWS

Il presente documento descrive i principali servizi cloud AWS utilizzati per il sistema Senonet.

Datacenter e infrastruttura di AWS

Il software è installato presso il cloud di Amazon, chiamato AWS (Amazon Web Services).

AWS detiene svariate certificazioni, tra cui HIPAA e ISO 27001; l'elenco completo è disponibile all'indirizzo http://aws.amazon.com/it/compliance/.

Il cloud AWS è una struttura mondiale con gerarchia geografica, il cui elemento principale sono le **Regioni**, Il numero delle regioni aumenta costantemente nel tempo e può essere visualizzato direttamente sul sito di AWS https://aws.amazon.com/it/about-aws/global-infrastructure/.

Una regione è un'area territoriale in cui si trovano diverse **Zone di disponibilità** (Availability Zone —AZ). Le AZ sono cluster di data center provvisti di alimentazione, rete e connettività ridondanti, ognuno in una propria struttura separata, attualmente esistono più di 80 zone di disponibilità (Availability Zone —AZ). All'interno delle AZ vengono eseguite applicazioni, database e altri servizi IT in ambienti di produzione con disponibilità, sicurezza, tolleranza ai guasti e scalabilità altrimenti impossibili da ottenere all'interno di un singolo data center.

In Europa sono presenti diverse regioni, Senonetwork utilizza la regione di Milano.

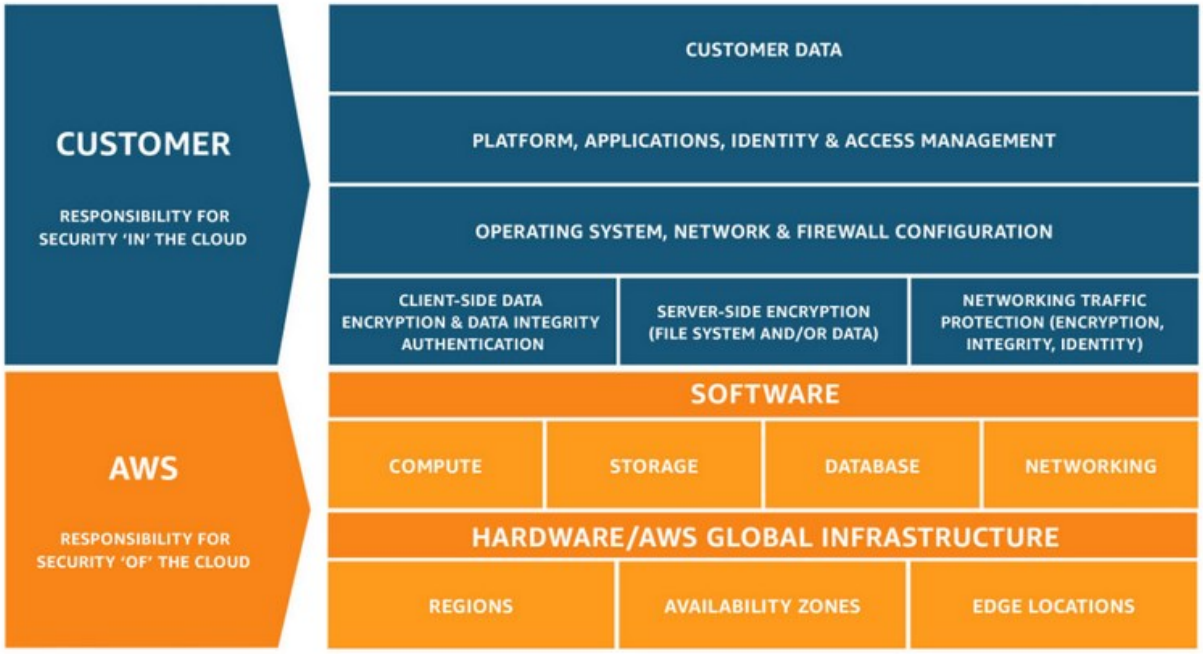
Per aumentare la flessibilità e il controllo nella gestione delle risorse, AWS utilizza i VPC (Virtual Private Cloud). I VPC sono unità logiche isolate, costituite da sottoreti, computer virtuali e altre risorse informatiche, associate a regole che ne controllano e limitano gli accessi. I VPC sono configurati dai partner e dai clienti in funzione delle esigenze delle applicazioni da utilizzare.

Sicurezza fisica e logica

Ogni data center utilizza avanzati sistemi di sorveglianza perimetrale e strettissimi controlli degli accessi da parte del personale AWS. Il personale che ha accesso fisico non ha accesso logico e viceversa.

La sicurezza è implementata secondo un modello a responsabilità suddivisa tra AWS, che gestisce i propri data center, e i clienti che utilizzano le risorse dei data center.

In tale modello AWS si occupa della sicurezza dell'infrastruttura globale, delle risorse hardware, della rete, della piattaforma di virtualizzazione e dei servizi gestiti, mentre i partner si occupano della sicurezza delle macchine virtuali (dal sistema operativo alle applicazioni) dei backup e delle regole dei firewall per l'accesso ai VPC. Amazon sottopone i data center a visite periodiche di controllo da parte di aziende indipendenti e specializzate nell'audit di infrastrutture informatiche e sicurezza.
https://aws.amazon.com/it/compliance/shared-responsibility-model/



Principali servizi utilizzati

VPC –Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) consente di effettuare il provisioning di una sezione logicamente isolata del cloud AWS, dove è possibile avviare risorse AWS in una rete virtuale definita dall'utente. Si ottiene così il controllo completo sull'ambiente virtuale di rete, incluse la selezione dell'intervallo di indirizzi IP, la creazione di sottoreti e la configurazione di tabelle di routing e di gateway di rete. VPC è compatibile fornisce accesso sicuro e comodo alle risorse e alle applicazioni con entrambi i protocolli IPv4 e IPv6.

Amazon VPC offre caratteristiche avanzate di sicurezza, ad esempio gruppi di sicurezza e liste di controllo degli accessi di rete, per ottenere il filtraggio in entrata e in uscita a livello di istanze e a livello di sottorete.

EC2 —Macchine virtuali per l'elaborazione

Elastic Cloud Computing (EC2) è un servizio che fornisce capacità di elaborazione sicura e scalabile nel cloud AWS. È concepito per rendere più semplice il cloud computing su scala Web. EC2 offre un ambiente molto affidabile, in cui le istanze di calcolo con vari sistemi operativi possono essere

avviate e gestite in modo rapido e prevedibile. Il servizio funziona all'interno dell'infrastruttura di reti e dei centri dati AWS. L'obiettivo del contratto sul livello di servizio di EC2 è raggiungere una disponibilità del 99,99% per ogni regione Amazon EC2.

EC2 funziona in combinazione con VPC per garantire sicurezza e funzionalità di rete resistenti per le risorse di calcolo.

S3 —Servizio di storage

Amazon S3 è uno storage di oggetti creato per memorizzare e ripristinare qualsiasi volume di dati da qualsiasi origine: siti Web, app mobili, applicazioni corporate e dati provenienti da dispositivi o sensori IoT. È stato progettato per offrire una durabilità del 99,999999999% e memorizzare dati per milioni di applicazioni utilizzate dai leader di mercato di ogni settore. S3 offre funzionalità di sicurezza e conformità che soddisfano anche le normative e i requisiti più severi.

Amazon S3 (Simple Storage Service) viene eseguito sull'infrastruttura cloud più grande al mondo. I dati nelle classi di storage Amazon S3, S3 Standard-IA e Amazon Glacier vengono distribuiti automaticamente su almeno tre zone di disponibilità fisiche a diversi chilometri l'una dall'altra all'interno della stessa regione AWS. Amazon S3 supporta tre diversi metodi di crittografia. S3 supporta inoltre diversi standard di sicurezza e certificazioni di conformità, tra cui PCI DSS, HIPAA/HITECH, FedRAMP, EU Data Protection Directive e FISMA, aiutando a soddisfare i requisiti di conformità per praticamente qualsiasi ente normativo in tutto il mondo.

IAM –Identity and Access Management

AWS IAM consente di gestire in sicurezza l'accesso ai servizi e alle risorse AWS. Grazie a IAM, è possibile creare e gestire utenti e gruppi AWS e utilizzare autorizzazioni per consentire o negare l'accesso alle risorse AWS. IAM consente di controllare l'accesso alle API del servizio AWS e di specificare le risorse. IAM consente inoltre di aggiungere condizioni specifiche, ad esempio l'ora del giorno, per controllare l'utilizzo di AWS da parte degli utenti, l'indirizzo IP di origine, l'eventuale uso del protocollo SSL oppure di un dispositivo con autenticazione a più fattori.

RDS –Relational Database Service

Amazon Relational Database Service (Amazon RDS) è un servizio di database con gestione automatizzata (AWS Automation). RDS fornisce una capacità ridimensionabile, automatizzando al tempo stesso le attività di amministrazione del database più onerose e complesse, quali il provisioning di hardware, l'impostazione di database, gli aggiornamenti e i backup. Consente di concentrarsi sulle proprie applicazioni per fornire le prestazioni ottimali, la disponibilità elevata, la sicurezza e la compatibilità di cui hanno bisogno. Senonetwork utilizza RDS configurato con la crittografia "At Rest" con chiavi gestite nel KMS.

KMS — Key Management Service

AWS Key Management Service (KMS) è un servizio per la sicurezza dei dati, si occupa della creazione e la gestione delle chiavi crittografiche e ne controlla l'utilizzo in una vasta gamma di servizi AWS e nelle tue applicazioni. AWS KMS è un servizio sicuro e resiliente che utilizza moduli di sicurezza hardware conformi agli standard FIPS 140-2 o in fase di conformità per proteggere le tue chiavi. AWS KMS è integrato inoltre con AWS CloudTrail, per fornire i registri dell'utilizzo di tutte le chiavi e soddisfare i requisiti normativi e di conformità.

CloudWatch —Raccolta e monitoraggio dei log

CloudWatch è un servizio di monitoraggio che fornisce dati e informazioni utili per monitorare le applicazioni per rispondere ai cambiamenti delle prestazioni a livello di sistema e ottimizzare l'utilizzo delle risorse. CloudWatch raccoglie dati operativi e di monitoraggio sotto forma di log, parametri ed eventi. È possibile ottenere una visione unificata dell'integrità operativa e una visibilità completa delle risorse, applicazioni e servizi AWS in esecuzione su AWS e on-premise. Si può utilizzare CloudWatch per rilevare comportamenti anomali, impostare allarmi, visualizzare log e parametri e intraprendere azioni automatiche.

AWS Backup —Gestione centralizzata e automazione dei backup

AWS Backup consente di centralizzare e automatizzare la protezione dei dati nei servizi AWS e nei carichi di lavoro ibridi. AWS Backup offre un servizio completamente gestito e basato su policy che semplifica ulteriormente la protezione dei dati su larga scala. AWS Backup permette di implementare a livello centrale le policy di protezione dei dati per configurare, gestire e governare l'attività di backup negli account e nelle risorse AWS.

ECR —Elastic Container Registry

Elastic Container Registry è un registro container completamente gestito che semplifica l'archiviazione, la gestione, la condivisione e la distribuzione delle immagini e degli artefatti del software. ECR supporta repository privati con autorizzazioni basate sulle risorse utilizzando AWS IAM. In questo modo gli utenti specificati o le istanze Amazon EC2 possono accedere ai repository e alle immagini dei container. È possibile inviare, estrarre e gestire immagini Docker, immagini Open Container Initiative (OCI) e artefatti compatibili con OCI.

Approfondimenti

Certificazioni	http://aws.amazon.com/it/compliance/
	https://aws.amazon.com/it/compliance/resources/
Sicurezza	http://aws.amazon.com/it/security/
GDPR	https://aws.amazon.com/it/compliance/gdpr-center/
S3	http://aws.amazon.com/it/s3/
EC2	https://aws.amazon.com/it/ec2/
VPC	https://aws.amazon.com/it/vpc/
RDS	https://aws.amazon.com/it/rds/
KMS	https://aws.amazon.com/it/kms/
CloudWatch	https://aws.amazon.com/it/cloudwatch/
AWS Backup	https://aws.amazon.com/it/backup/
ECR	https://aws.amazon.com/it/ecr/