Ridondanza Fisica e strategie di Disaster Recovery (DR)

E’ gestita attraverso l’infrastruttura di AWS che gestisce la sicurezza fisica e la ridondanza dei componenti hardware.

- **Regioni e Availability Zones (AZ)**: Ogni Regione è un'area geografica isolata che contiene più AZ. Ogni AZ è composta da uno o più data center fisicamente separati con alimentazione, connettività e raffreddamento ridondanti.
- **Connettività a bassa latenza**: Le AZ di una stessa Regione sono collegate tramite fibra ottica dedicata e ridondante, permettendo la **replica sincrona** dei dati.
- **Protezione Fisica**: I data center AWS includono controlli di accesso biometrici, sorveglianza 24/7 e sistemi avanzati di prevenzione incendi e UPS.

Componenti Chiave per il DR su AWS

- **Replicazione dei Dati**: Fondamentale per il DR. Backup dei dati su Amazon S3; ripristino manuale dell'infrastruttura in caso di disastro.

Strumenti per ottimizzare RTO e RPO

Per ridurre l'RPO (Protezione Dati)

- **AWS Backup:** Permette di centralizzare e automatizzare i backup di volumi EBS, database RDS e file system EFS con frequenze elevate (anche ogni ora).
- **Amazon S3 Replication:** Consente la replica automatica e asincrona degli oggetti tra diverse Regioni AWS (Cross-Region Replication).

Protezione Avanzata dell'Infrastruttura

Protezione Perimetrale e Anti-DDoS

AWS offre una difesa scalabile contro gli attacchi volumetrici e applicativi per garantire che l'infrastruttura rimanga disponibile.

- **AWS WAF (Web Application Firewall)**: Permette di creare regole personalizzate per bloccare pattern di attacco comuni come SQL Injection o Cross-Site Scripting (XSS) a livello applicativo (Layer 7).

Segmentazione e Isolamento di Rete

L'isolamento è fondamentale per limitare il "raggio d'azione" di un eventuale attacco.

- **Amazon VPC (Virtual Private Cloud)**: Crea una rete logica isolata dove l'utente ha il controllo totale su indirizzi IP, sottoreti e tabelle di instradamento.
- **Security Groups e Network ACL**: Fungono da firewall virtuali. I Security Groups sono stateful e controllano il traffico a livello di singola istanza, mentre le ACL sono stateless e controllano il

traffico a livello di intera sottorete.
- **AWS PrivateLink**: Permette di esporre servizi tra diverse VPC o verso internet in modo sicuro, senza che il traffico passi mai sulla rete pubblica.

Gestione degli Accessi Privilegiati

In un'infrastruttura avanzata, l'accesso ai server non avviene mai in modo diretto o insicuro.

- **AWS IAM (Identity and Access Management)**: Gestisce in modo granulare chi può fare cosa. Si applica il principio del **minimo privilegio**.
- **Multi-Factor Authentication (MFA)**: Obbligatoria per tutti gli accessi amministrativi, spesso tramite **Token OTP** o chiavi fisiche.

Monitoraggio e Rilevamento Minacce

La protezione non è completa senza la capacità di vedere cosa succede in tempo reale.

- **Amazon GuardDuty**: Un servizio di rilevamento delle minacce basato su machine learning che monitora costantemente i log (CloudTrail, VPC Flow Logs) alla ricerca di attività sospette o tentativi di intrusione.
- **AWS CloudTrail**: Registra ogni singola chiamata API effettuata nell'account, fornendo una traccia di audit completa per la conformità e l'analisi forense.
- **Amazon Inspector**: Esegue scansioni automatiche per rilevare vulnerabilità software o configurazioni di rete non sicure sulle istanze.

Crittografia e Protezione del Dato

Il dato deve essere protetto sia quando è fermo (at rest) sia quando si muove (in transit).

- **AWS KMS (Key Management Service)**: Gestisce le chiavi di crittografia utilizzate per proteggere i dischi (EBS), i database (RDS) e gli oggetti (S3).
- **Certificati SSL/TLS**: Gestiti tramite **AWS Certificate Manager (ACM)**, assicurano che le comunicazioni web siano sempre criptate con le versioni più recenti dei protocolli.

Standard di Qualità del Data Center

Gli standard di qualità dei data center di **AWS** si basano su un'infrastruttura progettata per superare i comuni requisiti di affidabilità industriale, supportata da decine di certificazioni globali e controlli fisici rigorosi.

A differenza di altri provider, AWS non segue una classificazione "Tier" rigida (come il sistema dell'Uptime Institute) per mantenere maggiore flessibilità nell'espansione e nel miglioramento delle performance, sebbene il suo design superi spesso gli standard di **Tier III e IV** in termini di manutenibilità e tolleranza ai guasti.

Ecco i principali standard e pilastri della qualità AWS:

Certificazioni di Qualità e Sicurezza Globale

AWS è sottoposta a verifiche periodiche da parte di auditor esterni indipendenti per confermare la conformità a standard internazionali:

- **ISO 9001**: Standard globale per la gestione della qualità.
- **ISO 27001 / 27017 / 27018**: Standard per la gestione della sicurezza delle informazioni, controlli specifici per il cloud e protezione dei dati personali.
- **SOC 1, 2 e 3**: Report sui controlli relativi a sicurezza, disponibilità e riservatezza.
- **PCI DSS Level 1**: Standard per la sicurezza dei dati dell'industria delle carte di pagamento.

Standard di Resilienza Fisica e Ambientale

La qualità dell'infrastruttura è garantita dalla scelta strategica dei siti e dalla ridondanza dei sistemi critici:

- **Selezione dei Siti**: AWS valuta rischi ambientali come inondazioni, attività sismica e condizioni meteorologiche estreme prima di costruire.
- **Ridondanza Energetica**: I sistemi di alimentazione elettrica sono progettati per essere completamente ridondanti e manutenibili senza impatto sulle operazioni 24/7.
- **Controllo Climatico**: Sistemi di monitoraggio costante della temperatura e dell'umidità per prevenire il surriscaldamento dell'hardware.
- **Prevenzione Incendi**: Utilizzo di sensori di rilevamento fumo avanzati e attrezzature di soppressione automatica in tutti gli ambienti critici.

Architettura a Zone di Disponibilità (AZ)

Lo standard qualitativo più elevato di AWS deriva dalla sua architettura logica:

- **Isolamento dei Guasti**: Ogni Regione AWS contiene più **Availability Zones** fisicamente distinte e indipendenti.
- **Infrastruttura Indipendente**: Ogni AZ dispone della propria alimentazione e rete ridondata, permettendo alle applicazioni di tollerare il guasto di un intero data center.

Protezione e Distruzione dei Dati

AWS applica standard rigorosi anche al ciclo di vita dei supporti fisici:

- **Media Destruction**: I dispositivi di memorizzazione guasti o obsoleti vengono smaltiti e distrutti secondo procedure che impediscono qualsiasi recupero di dati, in linea con standard come **NIST 800-88**.

Gestione degli Amministratori di Sistema

Procedure di controllo sul personale tecnico:

- **Autenticazione 2FA:** Obbligatoria per i dipendenti che accedono ai server via VPN.
- **Nomina e Istruzione**: Il personale è formalmente nominato "Amministratore di Sistema" secondo i provvedimenti del Garante Privacy.
- **Controllo Annuale**: L'operato degli amministratori è sottoposto a verifica ogni anno.

Service Level Agreement (SLA)

Service Level Agreement (SLA) - L’accesso alle applicazioni web SaaS è garantito con uno SLA al 99%, su base mensile, nelle seguenti fasce orarie:

- Giorni feriali: Dalle ore 08:00 alle ore 22:00
- Sabato e prefestivi: Dalle ore 08:00 alle ore 14:00

Nelle altre fasce orarie, incluse le festività nazionali, al fine di consentire le normali attività di manutenzione ordinaria e straordinaria, il servizio non è garantito.

Il Backup dei dati presenti nelle applicazioni web è richiedibile mezzo PEC aziendale; i dati saranno resi disponibili, entro 30 giorni dalla richiesta, mediante appositi link con scadenza a 30 giorni.