



Pratiche comprovate per lo sviluppo di una strategia multicloud

AWS Guida prescrittiva



AWS Guida prescrittiva: Pratiche comprovate per lo sviluppo di una strategia multicloud

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Introduzione	1
1. Allinea gli obiettivi multicloud alla tua strategia	3
Fusioni e acquisizioni	3
Desiderio di sfruttare le capacità differenziate a lungo termine di un altro CSP	3
Multicloud presso la holding e cloud primario presso la società operativa o il settore di business	4
2. Fai attenzione ai pregiudizi sul multicloud	6
Tutti stanno adottando strategie multicloud	6
Il multicloud riduce il rischio di dipendenza da un fornitore	6
Il multicloud migliora la disponibilità e la resilienza	7
Il multicloud offre prezzi migliori	8
3. Adottate una strategia e una governance chiare per sostenerla	11
4. Non distribuite carichi di lavoro contigui tra i cloud	13
5. Adottate una strategia di integrazione a lungo termine	14
6. Usa i contenitori in modo strategico	16
7. Hai una sola CCo E, ma specializzati al suo interno	17
8. Assicuratevi che la sicurezza sia sempre una priorità assoluta	19
9. Adottate un approccio 80/20 per una distribuzione equa	21
Conclusioni	23
Risorse	24
Cronologia dei documenti	25
Glossario	26
#	26
A	27
B	30
C	32
D	35
E	39
F	41
G	43
H	44
I	46
L	48
M	50

O	54
P	57
Q	59
R	60
S	63
T	67
U	68
V	69
W	69
Z	70
.....	lxxii

Pratiche comprovate per lo sviluppo di una strategia multicloud

Tom Godden ed Ellie Tamari, Amazon Web Services

Settembre 2025 ([storia del documento](#))

Oggi le organizzazioni si trovano ad affrontare messaggi contrastanti sull'adozione del multicloud. Alcuni lo sconsigliano del tutto, mentre altri sostengono che tutti stiano passando a un ambiente multicloud. La realtà si colloca tra questi due estremi: esistono ragioni legittime sia a favore che contro le strategie multicloud e il successo dipende dal bilanciamento del potenziale valore aziendale con la complessità e il rischio intrinseci.

At AWS, il nostro impegno per l'interoperabilità è uno dei motivi principali per cui molti clienti scelgono la nostra piattaforma. Crediamo nel darvi la libertà di innovare ovunque si trovino i vostri carichi di lavoro e nella possibilità di scegliere la tecnologia più adatta alle vostre esigenze. In AWS, siamo in prima linea nello sviluppo di soluzioni che consentono di creare e distribuire applicazioni in qualsiasi ambiente. Questo approccio incentrato sul cliente è fondamentale per la Cloud AWS, a cui si affidano milioni di clienti in tutto il mondo.

Comprendiamo che i clienti abbiano bisogno di piattaforme cloud che funzionino perfettamente sia con gli strumenti esistenti che con le scelte tecnologiche future. Non dovresti dover ricostruire tutto quando aggiungi funzionalità di un altro provider. Il tuo cloud dovrebbe aiutarti a connetterti, proteggere e gestire i carichi di lavoro in tutti gli ambienti senza costringerti a diventare un esperto in ogni piattaforma. AWS inserisce punti di connessione direttamente nei suoi servizi per aiutarti a operare in modo efficace, indipendentemente dal fatto che la tua strategia preveda l'uso AWS esclusivo o il seguire un approccio multicloud selettivo.

Riconosciamo che ogni organizzazione ha requisiti aziendali unici che guidano le decisioni relative alla strategia cloud. Che tu stia eseguendo carichi di lavoro principalmente su AWS, eseguendoli su più cloud o utilizzandoli AWS come parte di un'architettura multicloud più ampia, ci impegniamo ad aiutarti ad avere successo. AWS offre la profondità e l'ampiezza di strumenti e funzionalità per aiutarti a creare, migrare e operare con maggiore facilità e velocità, ovunque risiedano i tuoi carichi di lavoro. AWS gli strumenti semplificano la gestione tra i provider, massimizzando al contempo le prestazioni e il valore degli investimenti nel cloud.

Questo paper si concentra su principi comprovati per avere successo con una strategia multicloud, tra cui quando e dove un approccio multicloud ha senso e come AWS aiuta le aziende ad avere

successo con le loro strategie multicloud. Fornisce linee guida prescrittive per aiutare i dirigenti a fare scelte strategiche e decisionali informate relative all'adozione del multicloud. Questo paper non offre una discussione tecnica e approfondita sulle implementazioni multicloud. Per il supporto tecnico all'implementazione e l'assistenza per le vostre sfide specifiche, vi consigliamo di [collaborare con](#) il vostro architetto di soluzioni. AWS

Questo paper presenta nove principi comprovati per il successo del multicloud basati sulle nostre esperienze con AWS i clienti aziendali. Ogni principio affronta un aspetto critico della strategia multicloud, dall'allineamento degli obiettivi aziendali all'implementazione della sicurezza. Applicando questi principi, le organizzazioni possono affrontare la complessità del multicloud con sicurezza.

- [Principio 1. Allinea gli obiettivi multicloud alla tua strategia](#)
- [Principio 2. Fai attenzione ai pregiudizi sul multicloud](#)
- [Principio 3. Avere una strategia e una governance chiare per supportarlo](#)
- [Principio 4. Non distribuite carichi di lavoro contigui tra i cloud](#)
- [Principio 5. Avere una strategia di integrazione a lungo termine](#)
- [Principio 6. Usa i contenitori in modo strategico](#)
- [Principio 7. Hai una sola CCo E, ma sei specializzato](#)
- [Principio 8. Assicurati che la sicurezza sia sempre una priorità assoluta](#)
- [Principio 9. Adottate un approccio 80/20 per una distribuzione equa](#)

Principio 1. Allinea gli obiettivi multicloud alla tua strategia

La ricerca di Gartner e le tendenze del settore mostrano che le organizzazioni adottano sempre più approcci multicloud per soddisfare esigenze aziendali specifiche. I seguenti scenari dimostrano quando un'infrastruttura multicloud può essere strategicamente vantaggiosa.

Fusioni e acquisizioni

Le fusioni e le acquisizioni (M&A) creano decisioni immediate sulla strategia cloud. Sebbene la gestione di più cloud possa aumentare i costi e la complessità, un consolidamento rapido può ritardare il valore dell'integrazione e interrompere le operazioni aziendali. Le tue decisioni sul cloud diventano fondamentali per realizzare i vantaggi delle fusioni e acquisizioni.

La pianificazione dell'integrazione dovrebbe tenere conto dell'intero panorama tecnologico. Ogni carico di lavoro richiede una valutazione nel contesto della tempistica di integrazione e delle priorità aziendali.

La nostra guida:

- Sviluppa una strategia di consolidamento orientata al business che bilanci le esigenze di integrazione immediate con l'efficienza operativa a lungo termine. Mantieni inizialmente più cloud in circostanze in cui un consolidamento affrettato potrebbe interrompere le operazioni aziendali critiche o ritardare la realizzazione del valore delle fusioni e acquisizioni.
- Crea criteri di posizionamento dei carichi di lavoro chiari in linea con le tempistiche di integrazione. Dai priorità alle applicazioni che generano entrate e ai processi aziendali principali, tenendo conto delle dipendenze tecniche e dei requisiti operativi.

Desiderio di sfruttare le capacità differenziate a lungo termine di un altro CSP

La paura di perdere qualcosa spinge alcune aziende a desiderare un po' di ogni cloud. Le decisioni sul posizionamento dei carichi di lavoro influiscono sull'intera organizzazione, dai team di progettazione alle operazioni finanziarie fino alle operazioni di sicurezza.

Le organizzazioni devono quindi esaminare le motivazioni alla base della scelta di più cloud. Alcuni sostengono che ogni carico di lavoro dovrebbe risiedere sul provider di servizi cloud (CSP) che meglio soddisfa le sue esigenze. Tuttavia, l'ottimizzazione del carico di lavoro individuale deve essere

bilanciata con l'impatto organizzativo più ampio. Ogni ulteriore fornitore di servizi cloud rischia di aumentare la complessità operativa, creare nuovi requisiti di talenti e introdurre considerazioni sulla sicurezza che influiscono sull'intera organizzazione tecnologica.

La nostra guida:

- Segui un approccio 80/20: seleziona un provider principale per la maggior parte dei carichi di lavoro e prendi in considerazione fornitori aggiuntivi solo per casi d'uso specifici e di alto valore. Questa strategia massimizza l'efficienza e la fidelizzazione dei talenti riducendo al contempo la complessità.
- Considera il costo totale delle operazioni su cloud. Includi strumenti di sicurezza, prodotti di governance, sistemi di gestione finanziaria e sovraccarico operativo nella tua analisi.
- Valuta le dipendenze e le interazioni di ogni carico di lavoro. I carichi di lavoro raramente funzionano in modo isolato; condividono dati, controlli di sicurezza e processi operativi.
- Conduci un'analisi approfondita del rapporto prezzo/prestazioni tra i fornitori. Confrontate non solo i costi diretti, ma anche i costi generali della gestione di più ambienti.

Multicloud presso la holding e cloud primario presso la società operativa o il settore di business

Le società di private equity e le holding devono affrontare considerazioni specifiche sulla strategia cloud. Le società in portafoglio spesso mantengono strategie cloud indipendenti, spesso derivanti da attività di fusione e acquisizione passate. Questa struttura riduce la complessità tipicamente associata alle operazioni multicloud, poiché ogni unità aziendale opera in modo indipendente. Tuttavia, questa indipendenza può limitare le opportunità di usufruire degli sconti sui volumi e degli incentivi all'acquisto a livello aziendale.

L'efficacia della strategia cloud a livello di holding dipende dall'autonomia delle società in portafoglio e dalle loro esigenze tecnologiche individuali. Sebbene il consolidamento possa creare leva sugli acquisti, potrebbe entrare in conflitto con il modello operativo indipendente tipico delle holding e dei portafogli di private equity.

La nostra guida:

- Comprendi le strutture dei CSP Volume Discount. Ogni fornitore offre meccanismi per aggiungere o rimuovere filiali dagli accordi aziendali e suddividere le unità aziendali in entità separate. Si tratta di decisioni [bidirezionali](#).

- Pianifica attentamente gli impegni di acquisto nel cloud. Rivolgiti tempestivamente al team responsabile dell'account del tuo CSP oppure contatta un AWS Partner esperto in [AWS Cloud Operations per ricevere assistenza](#).
- Equilibra l'indipendenza con l'efficienza. Prendi in considerazione servizi condivisi o accordi di acquisto a vantaggio delle società in portafoglio senza limitarne l'operatività.
- Concentratevi innanzitutto sugli obiettivi aziendali. Sviluppa strategie tecnologiche che supportino il tuo modello operativo anziché perseguire una strategia multicloud fine a se stessa.
- Valuta le strategie cloud attraverso la lente della gestione del portafoglio. Considerate in che modo le scelte relative al cloud influiscono su potenziali cessioni o future acquisizioni.

Principio 2. Fai attenzione ai pregiudizi sul multicloud

Quando sviluppi la tua strategia multicloud, evita le idee sbagliate più comuni discusse nelle sezioni seguenti.

Tutti stanno adottando strategie multicloud

Le società di consulenza e le società di media dipingono un quadro complesso dell'adozione del multicloud. La ricerca mostra un ampio interesse per gli approcci multicloud, ma i modelli di spesa spesso raccontano una storia diversa. In pratica, molte aziende mantengono ambienti cloud singoli o relazioni chiare con i primary/secondary CSP. Questo divario evidenzia l'importanza di guardare oltre i titoli dei giornali e concentrarsi invece sulle esigenze specifiche dell'organizzazione.

La nostra guida:

- Prendi decisioni sul cloud in base ai tuoi requisiti aziendali specifici anziché seguire le tendenze del settore. Concentrati su costi e rischi misurabili per la tua organizzazione.
- Esamina i casi d'uso del multicloud nel tuo contesto di settore. Le strategie cloud che funzionano per le aziende di tecnologia di consumo potrebbero non tradursi in servizi finanziari, produzione o ambienti di gioco.
- Considerate la gravità dei dati come un fattore primario nelle decisioni relative al posizionamento dei carichi di lavoro. La posizione e lo spostamento dei dati spesso determinano l'architettura cloud più efficace.
- Vai oltre le statistiche sull'adozione per comprendere i modelli di spesa. Gli alti tassi di adozione del multicloud segnalati spesso mascherano i modelli di spesa effettivi.
- Valuta i vincoli tecnici prima di impegnarti in un ambiente multicloud. Alcuni carichi di lavoro offrono prestazioni migliori quando i componenti rimangono all'interno di un unico ambiente cloud.

Il multicloud riduce il rischio di dipendenza da un fornitore

La flessibilità dei fornitori è una considerazione legittima nello sviluppo di strategie cloud. Le organizzazioni apprezzano la capacità di adattare le proprie scelte tecnologiche all'evolversi delle esigenze aziendali. Questa preoccupazione riflette le esperienze precedenti con gli investimenti IT tradizionali che hanno creato impegni vincolanti a lungo termine. I servizi cloud offrono dinamiche diverse in merito alla flessibilità dei provider. AWS fornisce servizi compatibili con l'open source e opzioni di portabilità dei dati che riducono gli ostacoli tecnici alla migrazione. Tuttavia, il

compromesso tra flessibilità ed efficienza operativa rimane importante. Le organizzazioni devono soppesare il valore aziendale derivante dal mantenimento delle opzioni dei provider rispetto ai vantaggi tecnici di una profonda integrazione con i servizi specializzati di un fornitore primario.

Alcuni clienti cercano di evitare il lock-in progettando soluzioni indipendenti dal cloud che utilizzano contenitori. Questo approccio spesso li limita ai servizi di elaborazione e archiviazione di base e ignora i vantaggi delle funzionalità cloud avanzate. La nostra esperienza dimostra che questa strategia aggiunge una notevole complessità a causa dell'aumento dei tempi di sviluppo e delle risorse richieste rispetto all'utilizzo di servizi nativi.

La nostra guida:

- Considera il costo totale delle architetture indipendenti dal cloud. Il sovraccarico ingegneristico aggiuntivo potrebbe non giustificare i vantaggi in termini di portabilità.
- Utilizza le funzionalità native del cloud per ottenere il massimo valore. I soli servizi di elaborazione e archiviazione di base spesso sacrificano vantaggi significativi in termini di sicurezza, scalabilità e innovazione.
- Pianifica strategie cloud in base ai requisiti aziendali. Quando un'implementazione multicloud aggiunge un valore evidente, come la capacità di servire gli utenti su più piattaforme, l'investimento ingegneristico aggiuntivo diventa utile.
- Valuta scenari e costi di uscita realistici. Confronta la probabilità e i costi legati al cambio di fornitore con i vantaggi derivanti dall'utilizzo del set completo di Servizi AWS.
- Costruisci sulle basi open source di AWS i servizi gestiti come [Amazon Relational Database Service \(Amazon RDS\)](#) offrono flessibilità ed eccellenza operativa e supportano i motori di database che utilizzi oggi.
- Sfrutta gli strumenti di migrazione completi forniti da AWS. Ti aiutiamo a spostare i carichi di lavoro in qualsiasi direzione e forniamo il trasferimento gratuito dei dati in uscita se decidi di affidarti AWS ad altri provider. Per ulteriori informazioni, consulta il post del AWS blog [Trasferimento gratuito di dati su Internet quando ci si trasferisce da AWS](#).

Il multicloud migliora la disponibilità e la resilienza

La fiducia nel passaggio senza interruzioni del carico di lavoro tra i provider cloud durante le interruzioni spinge alcune organizzazioni verso strategie multicloud. Questa mentalità crea una visione eccessivamente semplificata della resilienza dell'infrastruttura cloud che ignora le realtà tecniche fondamentali.

Sulla base di anni di esperienza di lavoro con clienti multicloud AWS, abbiamo visto che il mantenimento della portabilità completa del carico di lavoro tra i provider spesso crea una notevole complessità senza offrire tutti i vantaggi previsti. Le applicazioni a uso intensivo di dati devono affrontare sfide insormontabili a causa dei vincoli di gravità dei dati. In effetti, a nostro avviso, è quasi impossibile per le organizzazioni implementare con successo un failover multicloud davvero fluido per carichi di lavoro con elevati volumi di dati.

Lydia Leong, illustre VP Analyst di Gartner, rafforza questa prospettiva in un [post sui social media](#): «Il failover multicloud è complesso e costoso al punto da essere quasi sempre impraticabile e non è un modo particolarmente efficace per affrontare i rischi di resilienza del cloud». La differenza intrinseca tra i provider di reti, storage, database, machine learning e sicurezza rende quasi impossibile la vera portabilità. La distribuzione dei carichi di lavoro tra i provider potrebbe aumentare il rischio, poiché un guasto in uno degli ambienti potrebbe causare un'interruzione in tutti gli ambienti.

La nostra guida:

- Concentrati sulla padronanza AWS delle funzionalità per i singoli carichi di lavoro invece di perseguire architetture multicloud complesse.
- Sviluppa la resilienza attraverso le zone di disponibilità invece di tentare il failover tra Regioni AWS diversi provider. Per un'analisi tecnica approfondita su come sia AWS possibile eseguire automaticamente il failover dei carichi di lavoro tra data center fisici, consulta il post del AWS blog, [Zonal autoshift — Automatic shift your traffic away](#) from Availability Zones when rileviamo potenziali problemi.
- Migra strategicamente i carichi di lavoro verso un'applicazione alla AWS volta e concentrati su un'applicazione alla volta per massimizzare il successo.

Il multicloud offre prezzi migliori

La competitività dei prezzi potrebbe essere l'argomento più debole di tutti a favore degli ambienti multicloud. Le esperienze delle organizzazioni con software complicati e costosi o contratti di data center che le vincolano a contratti pluriennali le hanno rese caute nell'approvvigionamento di servizi IT. Gli approcci di approvvigionamento tradizionali non si sono adattati agli pay-as-you-go acquisti, agli sconti sui volumi o alla realtà della concorrenza sui prezzi nel cloud. (A gennaio 2025, AWS ha ridotto i prezzi 151 volte sin dal suo inizio.)

Il principale fattore di riduzione dei costi è un ambiente cloud ben gestito e ottimizzato. Un'azienda ottiene una migliore ottimizzazione dei costi collaborando principalmente con un provider i cui servizi

offrono vantaggi in termini di rapporto prezzo/prestazioni (come le istanze di calcolo basate su chip progettati su misura come [AWS Graviton](#)) e dispone di soluzioni di gestione finanziaria cloud di qualità superiore. Secondo uno [studio del 2022 di Hackett Group su](#) oltre 1.000 organizzazioni, la spesa per l'infrastruttura come percentuale della spesa IT totale è stata inferiore del 20% per i clienti rispetto alle organizzazioni multicloud. AWS

La nostra esperienza ha dimostrato che le aziende non prevedono i costi aggiuntivi e la complessità derivanti dall'operatività su più cloud, né ponderano adeguatamente tale costo rispetto al guadagno percepito in un impegno di sourcing. head-to-head

La nostra guida:

- Sviluppa la tua strategia di ottimizzazione dei costi sulla base del pilastro di ottimizzazione dei costi di [AWS Well-Architected Framework](#). Esistono cinque principi di progettazione:
 - Implementa la gestione finanziaria nel cloud: per raggiungere il successo finanziario e accelerare la realizzazione del valore aziendale nel cloud, è necessario investire nella gestione finanziaria del cloud. La tua organizzazione deve dedicare il tempo e le risorse necessarie per creare le capacità in questo nuovo dominio di gestione della tecnologia e dell'utilizzo. Oltre alle capacità di sicurezza o operative, è necessario aumentare le capacità attraverso lo sviluppo di conoscenze, programmi, risorse e processi per contribuire a diventare un'organizzazione efficiente in termini di costi.
 - Adotta un modello a consumo: paga solo le risorse di calcolo che utilizzi e aumenta o riduci l'utilizzo in base alle necessità aziendali. Ad esempio, gli ambienti di sviluppo e test vengono in genere utilizzati solo per otto ore al giorno durante la settimana lavorativa. È possibile interrompere queste risorse quando non sono utilizzate per un potenziale risparmio sui costi del 75% (40 ore contro 168 ore).
 - Misura l'efficienza complessiva: misura la produttività aziendale del carico di lavoro e i costi associati alla consegna. Utilizza questi dati per comprendere i vantaggi ottenuti dall'incremento dell'output, dall'aumento della funzionalità e dalla riduzione dei costi.
 - Smettila di spendere soldi per il sollevamento indifferenziato di carichi pesanti: CSPs occupati delle operazioni del data center come scaffalature, impilamento e alimentazione dei server. Inoltre, eliminano l'onere operativo della gestione dei sistemi operativi e delle applicazioni utilizzando servizi gestiti. Ciò consente di concentrarsi sui clienti e sui progetti aziendali anziché sull'infrastruttura IT.
 - Analizza e attribuisce le spese: il cloud semplifica l'individuazione precisa di utilizzo e costi dei carichi di lavoro, permettendoti così di attribuire in modo trasparente i costi IT ai flussi di ricavi e ai singoli proprietari dei carichi di lavoro. In questo modo puoi misurare il ritorno sull'investimento

(ROI), mentre i proprietari dei carichi di lavoro hanno la possibilità di ottimizzare le risorse e ridurre i costi.

- Considerato il sovraccarico finanziario derivante dall'operare con diversi fornitori, invitiamo i clienti a investire pesantemente in strumenti di automazione e ottimizzazione dei costi. Ogni CSP offre numerosi strumenti nativi in quest'area, come il [Centrale ottimizzazione costi AWS](#). La maggior parte degli strumenti nativi offre funzionalità eccellenti ai clienti nel loro ambiente cloud. Tuttavia, per comprendere la spesa su più fronti CSPs, puoi scegliere tra un ricco set di prodotti ISV e SaaS (Software as a Service) che estendono queste funzionalità per fornire un'unica esperienza per l'ottimizzazione dei costi.
- La diluizione del potere d'acquisto attraverso una strategia di spending equity non genera valore aziendale. Può compromettere i potenziali sconti in termini di volume e potenzialmente compromettere la progettazione tecnica. Il modo più efficiente per utilizzare i servizi cloud consiste nell'utilizzare un provider principale per la maggior parte delle operazioni e utilizzarne altri CSPs solo laddove ciò aggiunga valore aziendale.

Principio 3. Avere una strategia e una governance chiare per supportarlo

Decidere di perseguire una strategia multicloud non è sufficiente; è necessario stabilire una strategia per raggiungere i propri obiettivi, inclusa una governance chiara su quali carichi di lavoro andranno dove e perché. È necessario utilizzare criteri di valutazione per ottimizzare i carichi di lavoro e le relative dipendenze. Se la valutazione viene lasciata ai singoli individui, un'espansione incontrollata e non coordinata potrebbe erodere CSPs il valore della strategia multicloud. Ti consigliamo di valutare regolarmente le prestazioni del carico di lavoro del CSP e di utilizzare la valutazione come input chiave per la selezione, i criteri e l'utilizzo futuro del CSP.

Una strategia di governance efficace richiede la visibilità sul numero totale di servizi, applicazioni e componenti utilizzati in tutta l'azienda. Parte integrante di ciò è una solida strategia di tagging che comprenda CSPs e stabilisca proprietà, utilizzo e ambiente chiari (ad esempio sviluppo, controllo qualità, allestimento e produzione) per tutte le risorse distribuite. Ogni elemento deve essere assegnato a un proprietario; se non è etichettato o se il proprietario non può essere identificato, deve essere rimosso. Lavoriamo a stretto contatto con un'importante organizzazione di servizi finanziari che trova e rimuove automaticamente tutte le risorse non etichettate e la considera una best practice, indipendentemente dagli inconvenienti che comporta per i team di sviluppo. Questo approccio di etichettatura codifica le regole di governance e ne automatizza l'applicazione anziché creare ostacoli al progresso (in altre parole, implementa barriere e non cancelli). I costi, le operazioni e la sicurezza devono essere tracciati, monitorati e gestiti allo stesso modo, con la stessa profondità di dati e la stessa trasparenza. CSPs

Quando si implementa una strategia multicloud, stabilire una struttura di account chiara e coerente tra i provider di cloud è fondamentale per mantenere il controllo operativo e la sicurezza. Ti consigliamo di adottare un hub-and-spoke modello che preveda la creazione di unità aziendali separate Account AWS per diverse unità aziendali. Queste sono gestite da due account centrali fondamentali: un security/audit account per il monitoraggio consolidato della conformità e della sicurezza e un account di rete centrale per la gestione dell'interconnettività. (Questo approccio è codificato nella progettazione di [AWS Control Tower](#). Tuttavia, i principi del privilegio minimo e della separazione dei compiti sono ugualmente applicabili ad altri cloud. Il [AWS Well-Architected Framework](#) discute a lungo questi concetti ed è altamente consigliato per il pubblico tecnico.) Questo approccio fondamentale dovrebbe essere rispecchiato in tutti i provider di servizi cloud per mantenere la coerenza nella governance e nelle operazioni. Gli account dei carichi di lavoro devono essere

organizzati per ambiente (sviluppo, allestimento, produzione) o funzione, con processi chiari per la creazione e l'eliminazione degli account.

La nostra guida:

- Implementa una strategia di tagging completa per mantenere chiari modelli di proprietà e utilizzo su tutte le risorse cloud. Tieni traccia degli ambienti, dei centri di costo, delle applicazioni e delle unità aziendali attraverso politiche di etichettatura coerenti. Rimuovi le risorse prive di tag appropriati per applicare gli standard di governance e mantenere la chiarezza dell'ambiente.
- Stabilisci un framework di conformità unificato che mappa i requisiti normativi in tutto il tuo ambiente multicloud. Conserva una documentazione chiara su come i controlli e le certificazioni di ciascun provider di cloud supportano i tuoi obblighi di conformità.
- Automatizza l'applicazione della governance tramite l'automazione anziché utilizzare processi di approvazione manuali. Codifica le tue regole di governance in sistemi automatizzati che impediscono le violazioni delle policy prima che si verifichino. Ciò elimina l'errore umano mantenendo al contempo la velocità di sviluppo.
- Struttura gli account in un hub-and-spoke modello con sicurezza centralizzata e controllo della rete. Crea account dedicati per il controllo della sicurezza e la gestione della rete per centralizzare le funzioni critiche. Questa base consente politiche di sicurezza e connettività di rete coerenti in tutta l'organizzazione.
- Per mantenere i limiti operativi, crea account, abbonamenti o progetti separati (a seconda della nomenclatura del CSP) per ambienti e funzioni diversi. Dividi i carichi di lavoro per ambienti di sviluppo, allestimento e produzione. Questa separazione impedisce la diffusione degli incidenti di sicurezza e mantiene chiari i domini operativi.
- Monitora i costi, le operazioni e la sicurezza attraverso metriche coerenti in tutto l'ambiente. Implementa il monitoraggio unificato dell'utilizzo delle risorse, degli eventi di sicurezza e dei modelli di spesa. Utilizza questi dati per ottimizzare il posizionamento dei carichi di lavoro e le decisioni di allocazione delle risorse.
- Impedisci l'utilizzo non autorizzato del cloud attraverso politiche organizzative e controlli automatizzati. Definisci processi chiari per la creazione di account e l'approvvigionamento delle risorse. Implementa [politiche di controllo del servizio \(SCPs\)](#) per far rispettare la conformità agli standard organizzativi in tutti gli account.
- Stabilisci controlli investigativi e preventivi per impedire che l'IT ombra emerga attraverso account di provider non autorizzati. Monitora l'utilizzo non autorizzato del cloud tramite note spese e traffico di rete. Blocca l'accesso non autorizzato dei provider mantenendo al contempo percorsi di innovazione approvati.

Principio 4. Non distribuite carichi di lavoro contigui tra i cloud

La distribuzione di carichi di lavoro contigui tra più provider cloud crea complessità, rischi e costi non necessari. Quando i carichi di lavoro che elaborano e analizzano i dati insieme riguardano più provider, le organizzazioni devono affrontare sfide in termini di spostamento, sincronizzazione e coerenza dei dati. I team devono utilizzare interfacce di gestione APIs, modelli di sicurezza e processi operativi diversi per ciascun provider, il che aumenta la probabilità di errori e aggiunge costi operativi. Questa complessità aumenta le possibilità di errori e di sovraccarico operativo e può ostacolare l'agilità e la scalabilità.

Tuttavia, in alcuni scenari pratici, le organizzazioni potrebbero dover distribuire carichi di lavoro contigui tra i cloud a causa di requisiti aziendali o tecnici specifici. In questi casi, ti consigliamo di stabilire criteri e principi guida chiari per valutare i compromessi e assicurarti che l'approccio sia in linea con la strategia multicloud complessiva dell'organizzazione.

Quando le organizzazioni scelgono di distribuire i carichi di lavoro su più cloud, l'adozione di un'architettura incentrata sulla messaggistica e sull'accoppiamento libero può alleviare molte delle sfide associate. Questo è il modo migliore per separare le preoccupazioni tra i cloud e ridurre l'ambito di impatto in caso di problemi di un provider. Le operazioni più soggette a vincoli temporali, come le transazioni finanziarie, dovrebbero idealmente essere conservate all'interno di un unico ambiente. Un'interruzione in un ambiente non dovrebbe mai mettere in pericolo i carichi di lavoro in un altro ambiente.

La nostra guida:

- Progetta carichi di lavoro cloud per l'indipendenza operativa per ridurre al minimo le dipendenze in tempo reale tra i provider. Quando è necessaria la distribuzione del carico di lavoro, implementa meccanismi efficienti di trasferimento di dati di massa invece di mantenere connessioni costanti tra cloud.
- Valuta ogni carico di lavoro distribuito proposto in base a criteri aziendali chiari. Considerate sia i vantaggi strategici che la complessità operativa introdotta dalla distribuzione.

Principio 5. Avere una strategia di integrazione a lungo termine

Fai attenzione quando sposti grandi volumi di dati tra applicazioni in cloud diversi, soprattutto se le risorse e le applicazioni di elaborazione sono distribuite in un CSP e le risorse di archiviazione dei dati sono distribuite in un altro. Una situazione del genere può aggiungere complessità e latenza che potrebbero compensare i vantaggi percepiti. Parliamo con molti clienti che dispongono di un data lake su un cloud ma desiderano eseguire l'apprendimento automatico (ML) o l'analisi con gli strumenti di un altro CSP. Decidere dove collocare i carichi di lavoro in un ambiente multicloud è una delle decisioni più cruciali, e spesso più impegnative, che le organizzazioni devono affrontare. Ti consigliamo di valutare ogni decisione sul posizionamento del carico di lavoro attraverso tre dimensioni critiche: requisiti tecnici, esigenze aziendali e punti di forza dei fornitori.

Inizia le valutazioni tecniche mappando le caratteristiche essenziali di ogni carico di lavoro: potenza di calcolo, operazioni sui dati, esigenze in termini di tempi di risposta e requisiti di crescita. Le applicazioni offrono naturalmente le migliori prestazioni quando si trovano vicino ai dati. L'allontanamento delle applicazioni dalle rispettive fonti di dati crea inutili ostacoli tecnici e rallenta le prestazioni.

Le decisioni aziendali devono tenere conto dei prezzi dei fornitori, dei requisiti di residenza dei dati e dei contratti con i fornitori. Ogni posizionamento del carico di lavoro influisce sulle operazioni, sulla sicurezza e sulla produttività dell'intera organizzazione. Considerare i carichi di lavoro in modo isolato porta a decisioni non ottimali.

La nostra guida:

- Implementa il trasferimento di massa di dati tra cloud anziché l'accesso in tempo reale. Pianifica l'aggiornamento periodico dei dati utilizzando operazioni di massa efficienti anziché utilizzare chiamate API costanti tra cloud. Questo approccio riduce i costi, migliora l'affidabilità e mantiene prestazioni costanti. Ad esempio, esporta dati riepilogativi sulle vendite giornaliere invece di interrogare le singole transazioni tra cloud.
- Considerate la gravità dei dati quando progettate il posizionamento dei carichi di lavoro. Mantieni le applicazioni vicine alle fonti di dati principali per mantenere le prestazioni e ridurre i costi. I modelli ML, i motori di analisi e i sistemi di elaborazione delle transazioni traggono tutti vantaggio dall'accesso diretto ai propri dati. L'allontanamento di questi carichi di lavoro dai relativi dati crea latenza e complessità di rete non necessarie.

- Valuta le decisioni relative al carico di lavoro nel contesto della tua strategia cloud completa invece di esaminarle isolatamente. Considerate in che modo ogni scelta di posizionamento influisce sui processi operativi, sui controlli di sicurezza e sulle capacità dei team all'interno dell'organizzazione. Una decisione che sembra ottimale per un singolo carico di lavoro potrebbe complicare il monitoraggio o aumentare i rischi per la sicurezza se vista in modo olistico.
- Definisci chiare politiche di proprietà e governance dei dati che specificano dove possono risiedere i diversi tipi di dati. Crea un framework di classificazione dei dati che favorisca decisioni coerenti sul posizionamento dei dati tra i provider di cloud.

Principio 6. Usa i contenitori in modo strategico

I container possono svolgere un ruolo importante nel supportare una strategia multicloud, ma è importante riconoscerne anche i limiti. L'uso dei container è generalmente una buona idea per qualsiasi applicazione moderna e nativa del cloud, poiché offrono vantaggi in termini di portabilità e coerenza tra diversi ambienti. I container sono indipendenti dalla piattaforma, il che significa che possono essere eseguiti su qualsiasi piattaforma o infrastruttura cloud che supporti la tecnologia di containerizzazione, come Kubernetes. Organizzazioni che utilizzano container possono sviluppare e impacchettare le proprie applicazioni una sola volta e poi distribuirle in modo coerente su più provider cloud o ambienti on-premise, senza la necessità di modifiche significative. Incapsulando il codice dell'applicazione, le dipendenze e l'ambiente di runtime all'interno di un container, puoi raggiungere un elevato grado di portabilità, che ti consente di spostare i carichi di lavoro senza problemi tra i provider di cloud o tra il cloud e i data center locali.

Tuttavia, i contenitori potrebbero non risolvere tutti i casi d'uso o eliminare tutte le sfide che un'organizzazione potrebbe dover affrontare nell'adozione di una strategia multicloud. I container funzionano meglio con architetture moderne basate su microservizi, ma potrebbero non essere altrettanto adatti per applicazioni monolitiche di grandi dimensioni. Inoltre, sebbene i container possano risolvere alcuni aspetti della portabilità, come il runtime delle applicazioni, non risolvono automaticamente i problemi relativi alla gestione dei dati, alle politiche di sicurezza e ad altre dipendenze tra cloud. Le organizzazioni devono ancora pianificare e progettare attentamente le proprie soluzioni multicloud per garantire una gestione coerente dei dati, controlli di sicurezza unificati e una perfetta integrazione tra componenti ospitati nel cloud e locali.

La nostra guida:

- Utilizza le funzionalità native di gestione dei container di ogni provider di servizi cloud per massimizzare il valore aziendale e accelerare la distribuzione. Questo approccio garantisce prestazioni ottimali evitando al contempo la complessità della creazione di soluzioni indipendenti dal cloud che raramente offrono rendimenti significativi.
- Sviluppa strategie di container che affrontino il quadro operativo completo, tra cui la gestione dei dati, la sicurezza e le dipendenze tra cloud. Concentrati sui risultati aziendali quando prendi decisioni sull'architettura dei container.

Principio 7. Hai una sola CCo E, ma sei specializzato

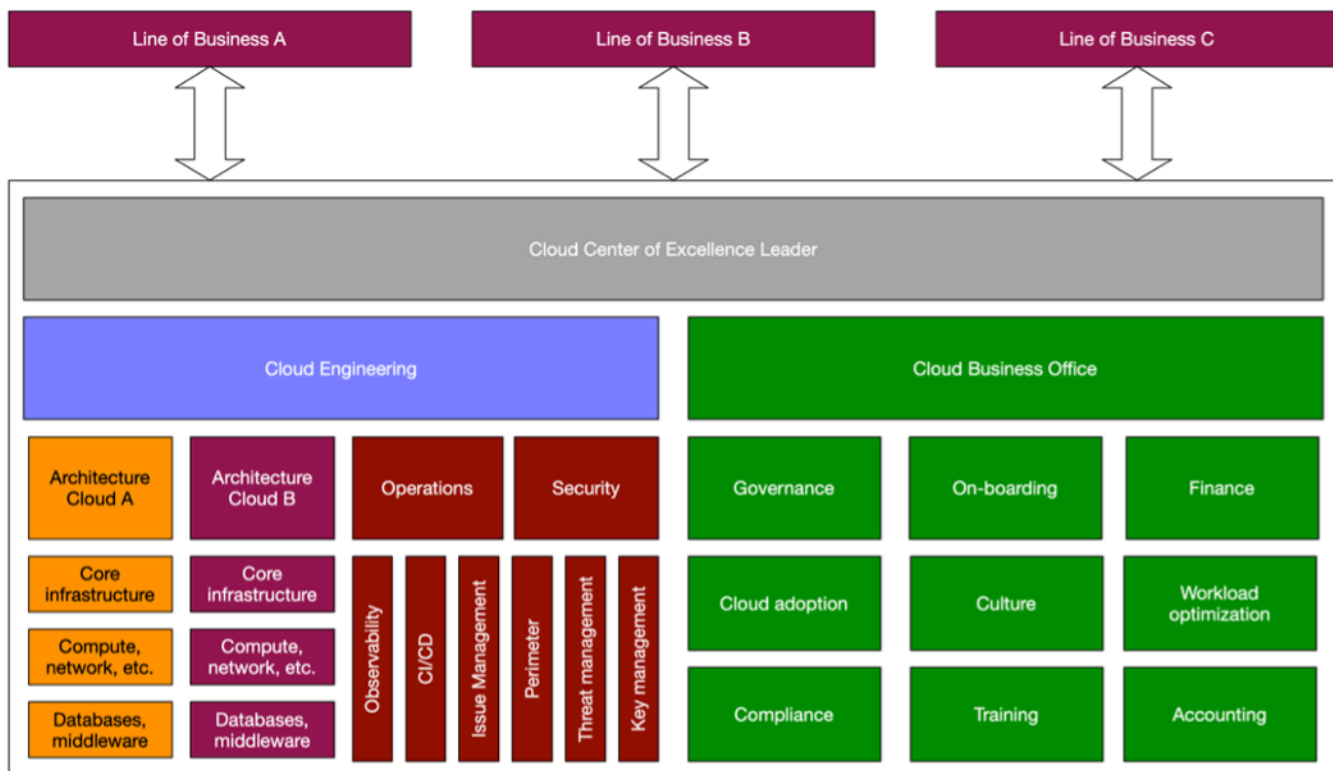
Come [consigliamo a molti AWS clienti](#), dovrete creare un Cloud Center of Excellence (CCoE) all'interno della vostra organizzazione per fornire leadership, standardizzazione e accelerazione del vostro percorso verso il cloud. Quando si tratta di ambienti multicloud, riteniamo che le aziende di maggior successo adottino un approccio equilibrato con E. CCo

Invece di stabilire CCo E separati per ogni CSP, ti consigliamo di avere un unico E unificato che CCo supervisioni la strategia multicloud dell'organizzazione. Questo aiuta a garantire un approccio coordinato e coerente anziché sforzi isolati che possono portare a divergenze, reingegnerizzazioni e sprechi. Assicurati che i team del tuo singolo CCo E dispongano delle competenze, degli strumenti e dei meccanismi specializzati necessari per ogni CSP utilizzato dalla tua organizzazione. Queste conoscenze specialistiche consentono all' CCoE di governare, supportare e accelerare l'uso delle diverse piattaforme cloud in modo efficace.

Ad esempio, la CCo E dovrebbe avere esperti AWS specifici che conoscano a fondo i servizi e le migliori pratiche, nonché esperti in grado di guidare l'organizzazione nell'uso di tali tecnologie cloud. Cloud AWS CSPs Questa competenza specializzata all'interno della singola CCo E può aiutare la tua organizzazione a trarre vantaggio dal coordinamento e dalla standardizzazione di un approccio centralizzato, garantendo al contempo che ogni piattaforma cloud venga utilizzata in modo ottimale.

La singola CCo E dovrebbe fungere da organo di governo centrale che stabilisce standard, politiche e best practice per la strategia multicloud dell'organizzazione. L'effettiva implementazione dei carichi di lavoro e dei progetti cloud può essere distribuita a team o unità aziendali specializzati, mentre il CCOE fornisce supervisione, supporto e coordinamento. Questo approccio equilibrato aiuta a garantire una strategia multicloud coesa, fornendo al contempo il necessario grado di flessibilità e autonomia all'interno dell'organizzazione.

Il diagramma seguente illustra come una CCo E può fornire un approccio e una governance centralizzati tra più linee di business (LOBs), team di progettazione del cloud e team di Cloud Business Office (CBO).



La nostra guida:

- Strutturate la vostra CCoE per mantenere la supervisione strategica, incorporando al contempo competenze specialistiche per ogni provider di servizi cloud. Concentrati sul reclutamento di competenze approfondite nelle singole piattaforme cloud invece di cercare rari specialisti multicloud e promuovi la condivisione interna delle conoscenze per sviluppare capacità organizzative.
- Consenti al tuo CCoE di stabilire standard a livello aziendale per questioni trasversali come la sicurezza e l'osservabilità, offrendo al contempo ai singoli team l'autonomia di eseguire le proprie attività nel rispetto di queste linee guida utilizzando strumenti e servizi nativi del cloud.
- Sviluppa una strategia completa per i talenti che bilanci una profonda esperienza nelle principali piattaforme cloud con una più ampia conoscenza dell'architettura. Concentrati sulla creazione di team che combinino solide competenze specifiche per il cloud con un'esperienza di architettura aziendale.

Principio 8. Assicuratevi che la sicurezza sia sempre una priorità assoluta

Un approccio multicloud rende più difficile garantire la sicurezza aumentando il rischio di accessi non autorizzati, perché il livello di sicurezza deve tenere conto di più superfici di attacco. Una strategia multicloud spesso costringe le aziende a gestire più modelli di sicurezza CSPs in aree come la gestione delle identità, la sicurezza della rete, la gestione degli asset e la registrazione degli audit. Questa complessità rischia di rendere più difficile la trasparenza, aumentare l'onere per i team di sicurezza e aumentare il rischio.

L'automazione della sicurezza è essenziale negli ambienti multicloud. La gestione delle identità deve funzionare senza problemi in tutti gli ambienti; deve connettere i provider di identità esistenti mantenendo politiche di accesso coerenti. La sicurezza richiede una protezione integrata tra i livelli di dati, rete ed endpoint. La classificazione dei dati, la crittografia e la gestione del ciclo di vita costituiscono le fondamenta. La sicurezza di rete si basa su design e schemi di connessione standardizzati. La protezione degli endpoint completa il framework attraverso una gestione coerente delle patch e controlli basati sull'host.

Questi elementi fondamentali sono fondamentali per l'adozione sicura e di successo di più provider cloud e devono essere considerati nelle prime fasi di qualsiasi pianificazione strategica multicloud.

La nostra guida:

- Implementa un framework di sicurezza integrato nel tuo ambiente multicloud incentrato su tre elementi principali: protezione dei dati tramite classificazione e crittografia standardizzate, sicurezza della rete attraverso modelli di progettazione coerenti e protezione degli endpoint tramite controlli sistematici e gestione delle patch.
- Stabilisci un modello operativo di sicurezza unificato che sfrutti le funzionalità di sicurezza native di ogni provider di cloud, mantenendo al contempo visibilità e controllo centralizzati attraverso strumenti e processi standardizzati.
- Centralizza la raccolta e l'analisi dei dati di sicurezza utilizzando [Amazon Security Lake](#). Questa piattaforma aggrega le informazioni di sicurezza provenienti da AWS altri provider di cloud, applicazioni SaaS e sistemi locali in un'unica visualizzazione. Supporta l'Open Cybersecurity Schema Framework (OCSF) e consente l'analisi standardizzata in un ambiente ibrido e multicloud. Questo approccio centralizzato migliora il rilevamento e la risposta alle minacce semplificando al contempo le operazioni di sicurezza.

- Implementa gli strumenti di sicurezza nativi di ciascun provider per migliorare le tue capacità di protezione. Questi servizi appositamente progettati riguardano le funzionalità specifiche del provider e restituiscono i dati alla piattaforma di sicurezza centralizzata. Una combinazione di strumenti nativi e visibilità centralizzata aiuta a fornire una copertura di sicurezza completa sull'intera infrastruttura.
- Implementa una strategia di osservabilità unificata che offra una visibilità completa sull'intero panorama cloud, compresi i dati operativi e di sicurezza, da zero. Standardizza gli approcci di monitoraggio leader del settore che consentono il monitoraggio coerente dei servizi aziendali indipendentemente da dove operano.
- Stabilisci standard a livello aziendale per la raccolta e la visualizzazione dei dati operativi che consentano l'identificazione e la risoluzione rapide dei problemi in un ambiente multicloud. Concentrati sulla creazione di un'unica fonte di verità per gli approfondimenti operativi che serva sia gli stakeholder tecnici che quelli aziendali.

Principio 9. Adottate un approccio 80/20 per una distribuzione equa

Il modo in cui distribuisce i carichi di lavoro tra i provider determina fundamentalmente il tuo successo nel multicloud. Molte organizzazioni perseguono erroneamente l'uguaglianza nella distribuzione sul cloud e cercano di distribuire i carichi di lavoro in modo uniforme tra i provider. Questo approccio aumenta la complessità senza offrire vantaggi proporzionali. Una distribuzione equa frammenta le capacità tecniche, diluisce il potere d'acquisto e crea costi operativi non necessari. I team hanno difficoltà a sviluppare competenze approfondite quando sono costretti a mantenere le competenze su più piattaforme contemporaneamente.

L'approccio 80/20 offre risultati dimostrabilmente migliori rispetto alla distribuzione equa tra i cloud. Concentrare l'80% del proprio investimento su un fornitore principale e utilizzare selettivamente gli altri per funzionalità specifiche crea una strategia bilanciata che riduce sia i costi che la complessità. Questo approccio concentrato accelera l'innovazione perché i team possono sviluppare competenze approfondite con i servizi avanzati della piattaforma principale. Il personale tecnico può diventare specializzato in un'unica architettura invece di mantenere una conoscenza superficiale in più ambienti. Quando gli ingegneri padroneggiano una piattaforma, creano in modo più efficiente, risolvono i problemi più rapidamente e implementano soluzioni più sofisticate.

Le aziende che seguono l'approccio 80/20 in genere segnalano una migliore fidelizzazione dei talenti perché i loro team sviluppano competenze preziose e commerciabili invece di essere limitati a più tecnologie. Questa strategia concentrata aiuta anche a semplificare la gestione della sicurezza limitando la complessità dei diversi modelli di sicurezza tra i diversi provider. Il cloud primario riceve la maggior parte degli investimenti in strumenti di sicurezza, soluzioni di monitoraggio e processi operativi. Ciò crea una base di sicurezza più solida di quella possibile con risorse equamente divise.

La nostra guida:

- Seleziona un provider cloud primario in linea con la maggior parte dei tuoi requisiti aziendali e tecnici. Questo provider dovrebbe supportare almeno l'80% dei tuoi carichi di lavoro e diventare la base della tua strategia cloud. Concentra gli investimenti in formazione, gli standard architetturici e i processi operativi sulla massimizzazione del valore di questa piattaforma principale.
- Sviluppa criteri chiari per i carichi di lavoro che giustifichino il posizionamento su cloud secondari. Questi criteri dovrebbero concentrarsi su un valore aziendale specifico che non può essere raggiunto dal provider principale. Evita di collocare i carichi di lavoro su cloud secondari semplicemente per mantenere l'equità di spesa o l'equilibrio artificiale tra i provider.

- Strutturate i vostri accordi aziendali in modo da rispecchiare il vostro approccio 80/20. Negozia sconti sulla base di volumi elevati con il tuo fornitore principale sulla base di una spesa concentrata e mantieni la flessibilità con i fornitori secondari per casi d'uso specifici. Questo approccio massimizza la leva di acquisto e in genere si traduce in prezzi complessivi migliori rispetto a una divisione equa della spesa.
- Allinea la tua strategia relativa ai talenti con il tuo approccio 80/20. Investi nello sviluppo di una profonda esperienza con i servizi del tuo fornitore principale, mantenendo al contempo una conoscenza sufficiente delle piattaforme secondarie per supportare carichi di lavoro specifici. Questa strategia mirata ai talenti migliora la produttività, accelera l'erogazione e riduce il rischio di carenze critiche nelle competenze.
- Misura regolarmente i risultati aziendali della tua strategia multicloud. Tieni traccia delle metriche che dimostrano il valore ottenuto da ciascun provider e, se necessario, modifica la distribuzione. L'obiettivo non è quello di evitare completamente il multicloud, ma di implementarlo strategicamente laddove carichi di lavoro specifici traggano davvero vantaggio da funzionalità esclusive di altri provider.

Conclusioni

Questo paper ha delineato nove principi chiave per lo sviluppo di una strategia multicloud efficace. Organizations ottiene il massimo successo attraverso un approccio cloud primario con l'uso strategico di provider aggiuntivi laddove esigenze aziendali specifiche lo richiedano. L'approccio 80/20 che abbiamo descritto bilancia l'attenzione con la flessibilità e consente alle organizzazioni di sviluppare competenze più approfondite, mantenere relazioni più solide con i fornitori e sviluppare talenti più preziosi, soddisfacendo al contempo i requisiti multicloud legittimi.

Un'implementazione multicloud di successo richiede una valutazione chiara delle esigenze aziendali anziché seguire le tendenze del settore. Le aziende devono stabilire una governance solida, mantenere la sicurezza come priorità assoluta, evitare di distribuire i carichi di lavoro connessi tra i provider, mantenere le applicazioni con i relativi dati transazionali, riconoscere i limiti dei container e mantenere un Cloud Center of Excellence unificato ma specializzato.

L' AWS approccio al cloud si basa fundamentalmente sulla scelta e sull'interoperabilità del cliente. Abbiamo progettato i nostri strumenti e servizi per funzionare senza problemi in tutti gli ambienti, perché sappiamo che le esigenze aziendali spesso non si limitano a un singolo fornitore. Dalle soluzioni di connettività ibride all'orchestrazione dei container che copre tutti gli ambienti, AWS offre funzionalità che aiutano a operare in modo efficace in tutto il panorama tecnologico.

Invece di obbligarvi a diventare esperti in più piattaforme, AWS semplifica la gestione multicloud attraverso strumenti intuitivi e interfacce coerenti. Ci concentriamo sulla rimozione della complessità in modo che tu possa concentrarti sull'innovazione. Queste funzionalità ti aiutano a implementare la tua strategia multicloud alle tue condizioni, sia che si tratti di utilizzare ambienti AWS esclusivi o specifici Servizi AWS insieme ad altri ambienti.

Il cloud dovrebbe potenziare la tua strategia aziendale, non limitarla. Applicando i principi delineati in questo paper e sfruttando le funzionalità di AWS interoperabilità, è possibile creare un approccio cloud che massimizzi il valore, riduca al minimo la complessità non necessaria e consenta all'organizzazione di avere successo a lungo termine nell'ambiente aziendale dinamico di oggi.

[Per saperne di più sulle AWS soluzioni che possono aiutare a semplificare la gestione in ambienti ibridi e multicloud, consulta Soluzioni per il multicloud.AWS](#)

Risorse

Riferimenti

- [Utilizzo di un Cloud Center of Excellence \(CCOE\) per trasformare l'intera azienda \(post sul blog\)](#)AWS
- [AWS Well-Architected Framework](#)
- [Identificazione delle opportunità con Cost Optimization Hub](#) (documentazione)AWS Cost Management
- [Il valore aziendale della migrazione ad Amazon Web Services](#) (The Hackett Group, febbraio 2022)
- [Trasferimento gratuito di dati su Internet quando si esce da AWS](#) (post AWS sul blog)

Strumenti

- [Trasferimento automatico zonale: sposta automaticamente il traffico lontano dalle zone di disponibilità quando rileviamo potenziali problemi](#) (post sul blog)AWS
- [AWS soluzioni per il multicloud](#)

AWS Partner

- [Cloud AWS Competenza operativa](#)

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un [feed RSS](#).

Modifica	Descrizione	Data
Pubblicazione iniziale	—	3 settembre 2025

AWS Glossario delle linee guida prescrittive

I seguenti sono termini di uso comune nelle strategie, nelle guide e nei modelli forniti da AWS Prescriptive Guidance. Per suggerire voci, utilizza il link [Fornisci feedback](#) alla fine del glossario.

Numeri

7 R

Sette strategie di migrazione comuni per trasferire le applicazioni sul cloud. Queste strategie si basano sulle 5 R identificate da Gartner nel 2011 e sono le seguenti:

- **Refactor/re-architect** — Sposta un'applicazione e modificala sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: migra il tuo database Oracle locale all'edizione Amazon PostgreSQL-Compatible Aurora.
- **Ridefinire la piattaforma (lift and reshape)**: trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale ad Amazon Relational Database Service (Amazon RDS) per Oracle in Cloud AWS
- **Riacquistare (drop and shop)**: passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: migra il tuo sistema di gestione delle relazioni con i clienti (CRM) su Salesforce.com
- **Eseguire il rehosting (lift and shift)**: trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale su Oracle su un'istanza EC2 in Cloud AWS
- **Trasferire (eseguire il rehosting a livello hypervisor)**: trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Esegui la migrazione dei server da una piattaforma locale a un servizio cloud per la stessa piattaforma. Esempio: migra un'applicazione su Microsoft Hyper-V. AWS
- **Riesaminare (mantenere)**: mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.
- **Ritirare**: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

A2A () Agent-to-Agent

Un protocollo statico per la collaborazione tra agenti che supporta la delega delle attività e il trasferimento dello stato.

ABAC

[Vedi controllo degli accessi basato sugli attributi.](#)

servizi astratti

Vedi [servizi gestiti](#).

ACIDO

Vedi [atomicità, consistenza, isolamento, durata](#).

migrazione attiva-attiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati (utilizzando uno strumento di replica bidirezionale o operazioni di doppia scrittura) ed entrambi i database gestiscono le transazioni provenienti dalle applicazioni di connessione durante la migrazione. Questo metodo supporta la migrazione in piccoli batch controllati anziché richiedere una conversione una tantum. È più flessibile ma richiede più lavoro rispetto alla migrazione [attiva-passiva](#).

migrazione attiva-passiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati, ma solo il database di origine gestisce le transazioni provenienti dalle applicazioni di connessione mentre i dati vengono replicati nel database di destinazione. Il database di destinazione non accetta alcuna transazione durante la migrazione.

Agente

Un sistema di intelligenza artificiale in grado di ragionare, pianificare e intraprendere azioni in modo autonomo utilizzando strumenti per raggiungere gli obiettivi.

Agente Ops

Pratiche operative per la creazione, il test, l'implementazione e l'esecuzione di agenti di intelligenza artificiale in produzione su larga scala.

funzione aggregata

Una funzione SQL che opera su un gruppo di righe e calcola un singolo valore restituito per il gruppo. Esempi di funzioni aggregate includono SUM e MAX.

Intelligenza artificiale

Vedi [intelligenza artificiale](#).

AIOps

Guarda le [operazioni di intelligenza artificiale](#).

anonimizzazione

Il processo di eliminazione permanente delle informazioni personali in un set di dati. L'anonimizzazione può aiutare a proteggere la privacy personale. I dati anonimi non sono più considerati dati personali.

anti-modello

Una soluzione utilizzata frequentemente per un problema ricorrente in cui la soluzione è controproducente, inefficace o meno efficace di un'alternativa.

controllo delle applicazioni

Un approccio alla sicurezza che consente l'uso solo di applicazioni approvate per proteggere un sistema dal malware.

portfolio di applicazioni

Una raccolta di informazioni dettagliate su ogni applicazione utilizzata da un'organizzazione, compresi i costi di creazione e manutenzione dell'applicazione e il relativo valore aziendale. Queste informazioni sono fondamentali per [il processo di scoperta e analisi del portfolio](#) e aiutano a identificare e ad assegnare la priorità alle applicazioni da migrare, modernizzare e ottimizzare.

intelligenza artificiale (IA)

Il campo dell'informatica dedicato all'uso delle tecnologie informatiche per svolgere funzioni cognitive tipicamente associate agli esseri umani, come l'apprendimento, la risoluzione di problemi e il riconoscimento di schemi. Per ulteriori informazioni, consulta la sezione [Che cos'è l'intelligenza artificiale?](#)

operazioni di intelligenza artificiale (AIOps)

Il processo di utilizzo delle tecniche di machine learning per risolvere problemi operativi, ridurre gli incidenti operativi e l'intervento umano e aumentare la qualità del servizio. Per ulteriori

informazioni su come viene utilizzato AIOps nella strategia di migrazione AWS , consulta la [guida all'integrazione delle operazioni](#).

crittografia asimmetrica

Un algoritmo di crittografia che utilizza una coppia di chiavi, una chiave pubblica per la crittografia e una chiave privata per la decrittografia. Puoi condividere la chiave pubblica perché non viene utilizzata per la decrittografia, ma l'accesso alla chiave privata deve essere altamente limitato.

atomicità, consistenza, isolamento, durabilità (ACID)

Un insieme di proprietà del software che garantiscono la validità dei dati e l'affidabilità operativa di un database, anche in caso di errori, interruzioni di corrente o altri problemi.

Controllo degli accessi basato su attributi (ABAC)

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, consulta [ABAC for AWS](#) nella documentazione AWS Identity and Access Management (IAM).

fonte di dati autorevole

Una posizione in cui è archiviata la versione principale dei dati, considerata la fonte di informazioni più affidabile. È possibile copiare i dati dalla fonte di dati autorevole in altre posizioni allo scopo di elaborarli o modificarli, ad esempio anonimizzandoli, oscurandoli o pseudonimizzandoli.

Zona di disponibilità

Una posizione distinta all'interno di un edificio Regione AWS che è isolata dai guasti in altre zone di disponibilità e offre una connettività di rete economica e a bassa latenza verso altre zone di disponibilità nella stessa regione.

AWS Cloud Adoption Framework (CAF)AWS

Un framework di linee guida e best practice AWS per aiutare le organizzazioni a sviluppare un piano efficiente ed efficace per passare con successo al cloud. AWS CAF organizza le linee guida in sei aree di interesse chiamate prospettive: business, persone, governance, piattaforma, sicurezza e operazioni. Le prospettive relative ad azienda, persone e governance si concentrano sulle competenze e sui processi aziendali; le prospettive relative alla piattaforma, alla sicurezza e alle operazioni si concentrano sulle competenze e sui processi tecnici. Ad esempio, la prospettiva relativa alle persone si rivolge alle parti interessate che gestiscono le risorse umane (HR), le funzioni del personale e la gestione del personale. In questa prospettiva, AWS CAF fornisce linee guida per lo sviluppo delle persone, la formazione e le comunicazioni per aiutare a preparare

l'organizzazione all'adozione del cloud di successo. Per ulteriori informazioni, consulta il [sito web di AWS CAF](#) e il [white paper AWS CAF](#).

AWS Workload Qualification Framework (WQF)AWS

Uno strumento che valuta i carichi di lavoro di migrazione dei database, consiglia strategie di migrazione e fornisce stime del lavoro. AWS WQF è incluso in (). AWS Schema Conversion Tool AWS SCT Analizza gli schemi di database e gli oggetti di codice, il codice dell'applicazione, le dipendenze e le caratteristiche delle prestazioni e fornisce report di valutazione.

B

bot difettoso

Un [bot](#) che ha lo scopo di disturbare o causare danni a individui o organizzazioni.

BCP

Vedi la [pianificazione della continuità operativa](#).

grafico comportamentale

Una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni nel tempo. Puoi utilizzare un grafico comportamentale con Amazon Detective per esaminare tentativi di accesso non riusciti, chiamate API sospette e azioni simili. Per ulteriori informazioni, consulta [Dati in un grafico comportamentale](#) nella documentazione di Detective.

sistema big-endian

Un sistema che memorizza per primo il byte più importante. Vedi anche [endianness](#).

Classificazione binaria

Un processo che prevede un risultato binario (una delle due classi possibili). Ad esempio, il modello di machine learning potrebbe dover prevedere problemi come "Questa e-mail è spam o non è spam?" o "Questo prodotto è un libro o un'auto?"

filtro Bloom

Una struttura di dati probabilistica ed efficiente in termini di memoria che viene utilizzata per verificare se un elemento fa parte di un set.

blue/green dispiegamento

Una strategia di implementazione in cui si creano due ambienti separati ma identici. La versione corrente dell'applicazione viene eseguita in un ambiente (blu) e la nuova versione dell'applicazione nell'altro ambiente (verde). Questa strategia consente di ripristinare rapidamente il sistema con un impatto minimo.

bot

Un'applicazione software che esegue attività automatizzate su Internet e simula l'attività o l'interazione umana. Alcuni bot sono utili o utili, come i web crawler che indicizzano le informazioni su Internet. Alcuni altri bot, noti come bot dannosi, hanno lo scopo di disturbare o causare danni a individui o organizzazioni.

botnet

Reti di [bot](#) infettate da [malware](#) e controllate da un'unica parte, nota come bot herder o bot operator. Le botnet sono il meccanismo più noto per scalare i bot e il loro impatto.

ramo

Un'area contenuta di un repository di codice. Il primo ramo creato in un repository è il ramo principale. È possibile creare un nuovo ramo a partire da un ramo esistente e quindi sviluppare funzionalità o correggere bug al suo interno. Un ramo creato per sviluppare una funzionalità viene comunemente detto ramo di funzionalità. Quando la funzionalità è pronta per il rilascio, il ramo di funzionalità viene ricongiunto al ramo principale. Per ulteriori informazioni, consulta [Informazioni sulle filiali](#) (documentazione). GitHub

accesso break-glass

In circostanze eccezionali e tramite una procedura approvata, un mezzo rapido per consentire a un utente di accedere a un sito a Account AWS cui in genere non dispone delle autorizzazioni necessarie. Per ulteriori informazioni, consulta l'indicatore [Implementare le procedure break-glass](#) nella guida. AWS Well-Architected

strategia brownfield

L'infrastruttura esistente nell'ambiente. Quando si adotta una strategia brownfield per un'architettura di sistema, si progetta l'architettura in base ai vincoli dei sistemi e dell'infrastruttura attuali. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e [greenfield](#).

cache del buffer

L'area di memoria in cui sono archiviati i dati a cui si accede con maggiore frequenza.

capacità di business

Azioni intraprese da un'azienda per generare valore (ad esempio vendite, assistenza clienti o marketing). Le architetture dei microservizi e le decisioni di sviluppo possono essere guidate dalle capacità aziendali. Per ulteriori informazioni, consulta la sezione [Organizzazione in base alle funzionalità aziendali](#) del whitepaper [Esecuzione di microservizi containerizzati su AWS](#).

pianificazione della continuità operativa (BCP)

Un piano che affronta il potenziale impatto di un evento che comporta l'interruzione dell'attività, come una migrazione su larga scala, sulle operazioni e consente a un'azienda di riprendere rapidamente le operazioni.

C

CAF

Vedi [AWS Cloud Adoption Framework](#).

implementazione canaria

Il rilascio lento e incrementale di una versione agli utenti finali. Quando sei sicuro, distribuisce la nuova versione e sostituisci la versione corrente nella sua interezza.

CoE

Vedi [Cloud Center of Excellence](#).

CDC

Vedi [Change Data Capture](#).

Change Data Capture (CDC)

Il processo di tracciamento delle modifiche a un'origine dati, ad esempio una tabella di database, e di registrazione dei metadati relativi alla modifica. È possibile utilizzare CDC per vari scopi, ad esempio il controllo o la replica delle modifiche in un sistema di destinazione per mantenere la sincronizzazione.

ingegneria del caos

Introduzione intenzionale di guasti o eventi dirompenti per testare la resilienza di un sistema. Puoi usare [AWS Fault Injection Service \(AWS FIS\)](#) per eseguire esperimenti che stressano i tuoi AWS carichi di lavoro e valutarne la risposta.

CI/CD

Vedi [integrazione continua e distribuzione continua](#).

classificazione

Un processo di categorizzazione che aiuta a generare previsioni. I modelli di ML per problemi di classificazione prevedono un valore discreto. I valori discreti sono sempre distinti l'uno dall'altro. Ad esempio, un modello potrebbe dover valutare se in un'immagine è presente o meno un'auto.

Sviluppatore cittadino

Un utente aziendale che crea applicazioni di intelligenza artificiale utilizzando piattaforme senza code/low codice senza competenze tecniche specializzate.

crittografia lato client

Crittografia dei dati localmente, prima che il bersaglio li Servizio AWS riceva.

centro di eccellenza del cloud (CCoE)

Un team multidisciplinare che guida le iniziative di adozione del cloud in tutta l'organizzazione, tra cui lo sviluppo di best practice per il cloud, la mobilitazione delle risorse, la definizione delle tempistiche di migrazione e la guida dell'organizzazione attraverso trasformazioni su larga scala. Per ulteriori informazioni, consulta i [post di CCoE](#) sull' Cloud AWS Enterprise Strategy Blog.

cloud computing

La tecnologia cloud generalmente utilizzata per l'archiviazione remota di dati e la gestione dei dispositivi IoT. Il cloud computing è generalmente collegato alla tecnologia di [edge computing](#).

modello operativo cloud

In un'organizzazione IT, il modello operativo utilizzato per creare, maturare e ottimizzare uno o più ambienti cloud. Per ulteriori informazioni, consulta [Building your Cloud Operating Model](#).

fasi di adozione del cloud

Le quattro fasi che le organizzazioni in genere attraversano quando migrano verso Cloud AWS:

- Progetto: esecuzione di alcuni progetti relativi al cloud per scopi di dimostrazione e apprendimento
- Fondamento: effettuare investimenti fondamentali per dimensionare l'adozione del cloud (ad esempio, creazione di una zona di destinazione, definizione di un CCoE, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni

- Re-invention — Ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post del blog [The Journey Toward Cloud-First & the Stages of Adoption](#) sul blog Enterprise Strategy. Cloud AWS Per informazioni sulla loro relazione con la strategia di AWS migrazione, consulta la guida alla [preparazione alla migrazione](#).

CMDB

Vedi [database di gestione della configurazione](#).

repository di codice

Una posizione in cui il codice di origine e altri asset, come documentazione, esempi e script, vengono archiviati e aggiornati attraverso processi di controllo delle versioni. Gli archivi cloud più comuni includono GitHub o Bitbucket Cloud. Ogni versione del codice è denominata ramo. In una struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola CI/CD pipeline può utilizzare più repository.

cache fredda

Una cache del buffer vuota, non ben popolata o contenente dati obsoleti o irrilevanti. Ciò influisce sulle prestazioni perché l'istanza di database deve leggere dalla memoria o dal disco principale, il che richiede più tempo rispetto alla lettura dalla cache del buffer.

dati freddi

Dati a cui si accede raramente e che in genere sono storici. Quando si eseguono interrogazioni di questo tipo di dati, le interrogazioni lente sono in genere accettabili. Lo spostamento di questi dati su livelli o classi di storage meno costosi e con prestazioni inferiori può ridurre i costi.

visione artificiale (CV)

Un campo dell'[intelligenza artificiale](#) che utilizza l'apprendimento automatico per analizzare ed estrarre informazioni da formati visivi come immagini e video digitali. Ad esempio, Amazon SageMaker AI fornisce algoritmi di elaborazione delle immagini per CV.

deriva della configurazione

Per un carico di lavoro, una modifica della configurazione rispetto allo stato previsto. Potrebbe causare la non conformità del carico di lavoro e in genere è graduale e involontaria.

database di gestione della configurazione (CMDB)

Un repository che archivia e gestisce le informazioni su un database e il relativo ambiente IT, inclusi i componenti hardware e software e le relative configurazioni. In genere si utilizzano i dati di un CMDB nella fase di individuazione e analisi del portafoglio della migrazione.

Pacchetto di conformità

Una raccolta di AWS Config regole e azioni correttive che puoi assemblare per personalizzare i controlli di conformità e sicurezza. È possibile distribuire un pacchetto di conformità come singola entità in una regione Account AWS and o all'interno di un'organizzazione utilizzando un modello YAML. Per ulteriori informazioni, consulta i [Conformance Pack](#) nella documentazione. AWS Config

integrazione e distribuzione continue () CI/CD

Il processo di automazione delle fasi di origine, compilazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD viene comunemente descritto come una pipeline. CI/CD può aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le consegne. Per ulteriori informazioni, consulta [Vantaggi della distribuzione continua](#). CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta [Distribuzione continua e implementazione continua a confronto](#).

CV

Vedi [visione artificiale](#).

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

Un processo per identificare e classificare i dati nella rete in base alla loro criticità e sensibilità. È un componente fondamentale di qualsiasi strategia di gestione dei rischi di sicurezza informatica perché consente di determinare i controlli di protezione e conservazione appropriati per i dati. La classificazione dei dati è un componente del pilastro della sicurezza nel AWS Well-Architected Framework. Per ulteriori informazioni, consulta [Classificazione dei dati](#).

deriva dei dati

Una variazione significativa tra i dati di produzione e i dati utilizzati per addestrare un modello di machine learning o una modifica significativa dei dati di input nel tempo. La deriva dei dati può ridurre la qualità, l'accuratezza e l'equità complessive nelle previsioni dei modelli ML.

dati in transito

Dati che si spostano attivamente attraverso la rete, ad esempio tra le risorse di rete.

rete di dati

Un framework architettonico che fornisce la proprietà distribuita e decentralizzata dei dati con gestione e governance centralizzate.

riduzione al minimo dei dati

Il principio della raccolta e del trattamento dei soli dati strettamente necessari. Praticare la riduzione al minimo dei dati in the Cloud AWS può ridurre i rischi per la privacy, i costi e l'impronta di carbonio delle analisi.

perimetro dei dati

Una serie di barriere preventive nell' AWS ambiente che aiutano a garantire che solo le identità attendibili accedano alle risorse attendibili delle reti previste. Per ulteriori informazioni, consulta [Building a data perimeter](#) on AWS.

pre-elaborazione dei dati

Trasformare i dati grezzi in un formato che possa essere facilmente analizzato dal modello di ML. La pre-elaborazione dei dati può comportare la rimozione di determinate colonne o righe e l'eliminazione di valori mancanti, incoerenti o duplicati.

provenienza dei dati

Il processo di tracciamento dell'origine e della cronologia dei dati durante il loro ciclo di vita, ad esempio il modo in cui i dati sono stati generati, trasmessi e archiviati.

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

Un sistema di gestione dei dati che supporta la business intelligence, come l'analisi. I data warehouse contengono in genere grandi quantità di dati storici e vengono generalmente utilizzati per interrogazioni e analisi.

linguaggio di definizione del database (DDL)

Istruzioni o comandi per creare o modificare la struttura di tabelle e oggetti in un database.

linguaggio di manipolazione del database (DML)

Istruzioni o comandi per modificare (inserire, aggiornare ed eliminare) informazioni in un database.

DDL

Vedi linguaggio di [definizione del database](#).

deep ensemble

Combinare più modelli di deep learning per la previsione. È possibile utilizzare i deep ensemble per ottenere una previsione più accurata o per stimare l'incertezza nelle previsioni.

deep learning

Un sottocampo del ML che utilizza più livelli di reti neurali artificiali per identificare la mappatura tra i dati di input e le variabili target di interesse.

difesa in profondità

Un approccio alla sicurezza delle informazioni in cui una serie di meccanismi e controlli di sicurezza sono accuratamente stratificati su una rete di computer per proteggere la riservatezza, l'integrità e la disponibilità della rete e dei dati al suo interno. Quando si adotta questa strategia AWS, si aggiungono più controlli a diversi livelli della AWS Organizations struttura per proteggere le risorse. Ad esempio, un approccio di difesa approfondita potrebbe combinare autenticazione a più fattori, segmentazione della rete e crittografia.

amministratore delegato

In AWS Organizations, un servizio compatibile può registrare un account AWS membro per amministrare gli account dell'organizzazione e gestire le autorizzazioni per quel servizio. Questo account è denominato amministratore delegato per quel servizio specifico. Per ulteriori informazioni e un elenco di servizi compatibili, consulta [Servizi che funzionano con AWS Organizations](#) nella documentazione di AWS Organizations .

implementazione

Il processo di creazione di un'applicazione, di nuove funzionalità o di correzioni di codice disponibili nell'ambiente di destinazione. L'implementazione prevede l'applicazione di modifiche in una base di codice, seguita dalla creazione e dall'esecuzione di tale base di codice negli ambienti applicativi.

Ambiente di sviluppo

[Vedi ambiente](#).

controllo di rilevamento

Un controllo di sicurezza progettato per rilevare, registrare e avvisare dopo che si è verificato un evento. Questi controlli rappresentano una seconda linea di difesa e avvisano l'utente in caso di eventi di sicurezza che aggirano i controlli preventivi in vigore. Per ulteriori informazioni, consulta [Controlli di rilevamento](#) in Implementazione dei controlli di sicurezza in AWS.

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

Una rappresentazione virtuale di un sistema reale, ad esempio un edificio, una fabbrica, un'attrezzatura industriale o una linea di produzione. I gemelli digitali supportano la manutenzione predittiva, il monitoraggio remoto e l'ottimizzazione della produzione.

tabella delle dimensioni

In uno [schema a stella](#), una tabella più piccola che contiene gli attributi dei dati quantitativi in una tabella dei fatti. Gli attributi della tabella delle dimensioni sono in genere campi di testo o numeri discreti che si comportano come testo. Questi attributi vengono comunemente utilizzati per il vincolo delle query, il filtraggio e l'etichettatura dei set di risultati.

disastro

Un evento che impedisce a un carico di lavoro o a un sistema di raggiungere gli obiettivi aziendali nella sua sede principale di implementazione. Questi eventi possono essere disastri naturali, guasti tecnici o il risultato di azioni umane, come errori di configurazione involontari o attacchi di malware.

disaster recovery (DR)

La strategia e il processo utilizzati per ridurre al minimo i tempi di inattività e la perdita di dati causati da un [disastro](#). Per ulteriori informazioni, consulta [Disaster Recovery of Workload su AWS: Recovery in the Cloud in the AWS Well-Architected Framework](#).

DML

Vedi linguaggio di [manipolazione del database](#).

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro *Domain-Driven Design: Tackling Complexity in the Heart of Software* (Boston: Addison-Wesley Professional, 2003). Per informazioni su come utilizzare la progettazione basata sul dominio con lo *strangler fig pattern*, consulta [Modernizzare i servizi Web Microsoft ASP.NET \(ASMX\) legacy in modo incrementale utilizzando contenitori e Amazon API Gateway](#).

DOTT.

Vedi [disaster recovery](#).

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, puoi utilizzarlo AWS CloudFormation per [rilevare la deriva nelle risorse di sistema](#) oppure puoi usarlo AWS Control Tower per [rilevare cambiamenti nella tua landing zone](#) che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la [mappatura del flusso di valore dello sviluppo](#).

E

EDA

Vedi [analisi esplorativa dei dati](#).

MODIFICA

Vedi [scambio elettronico di dati](#).

edge computing

La tecnologia che aumenta la potenza di calcolo per i dispositivi intelligenti all'edge di una rete IoT. Rispetto al [cloud computing](#), [l'edge computing](#) può ridurre la latenza di comunicazione e migliorare i tempi di risposta.

scambio elettronico di dati (EDI)

Lo scambio automatizzato di documenti aziendali tra organizzazioni. Per ulteriori informazioni, vedere [Cos'è lo scambio elettronico di dati](#).

crittografia

Un processo di elaborazione che trasforma i dati in chiaro, leggibili dall'uomo, in testo cifrato.

chiave crittografica

Una stringa crittografica di bit randomizzati generata da un algoritmo di crittografia. Le chiavi possono variare di lunghezza e ogni chiave è progettata per essere imprevedibile e univoca.

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. Big-endian i sistemi memorizzano per primi il byte più importante. Little-endian i sistemi memorizzano per primi il byte meno importante.

endpoint

Vedi [service endpoint](#).

servizio endpoint

Un servizio che puoi ospitare in un cloud privato virtuale (VPC) da condividere con altri utenti. Puoi creare un servizio endpoint con AWS PrivateLink e concedere autorizzazioni ad altri Account AWS o a AWS Identity and Access Management (IAM) principali. Questi account o principali possono connettersi al servizio endpoint in privato creando endpoint VPC di interfaccia. Per ulteriori informazioni, consulta [Creazione di un servizio endpoint](#) nella documentazione di Amazon Virtual Private Cloud (Amazon VPC).

pianificazione delle risorse aziendali (ERP)

Un sistema che automatizza e gestisce i processi aziendali chiave (come contabilità, [MES](#) e gestione dei progetti) per un'azienda.

crittografia envelope

Il processo di crittografia di una chiave di crittografia con un'altra chiave di crittografia. Per ulteriori informazioni, vedete [Envelope encryption](#) nella documentazione AWS Key Management Service (AWS KMS).

ambiente

Un'istanza di un'applicazione in esecuzione. Di seguito sono riportati i tipi di ambiente più comuni nel cloud computing:

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono

utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.

- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.
- ambiente di produzione: un'istanza di un'applicazione in esecuzione a cui gli utenti finali possono accedere. In una CI/CD pipeline, l'ambiente di produzione è l'ultimo ambiente di distribuzione.
- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione. Ad esempio, le epiche della sicurezza AWS CAF includono la gestione delle identità e degli accessi, i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS , consulta la [guida all'implementazione del programma](#).

ERP

Vedi [pianificazione delle risorse aziendali](#).

analisi esplorativa dei dati (EDA)

Il processo di analisi di un set di dati per comprenderne le caratteristiche principali. Si raccolgono o si aggregano dati e quindi si eseguono indagini iniziali per trovare modelli, rilevare anomalie e verificare ipotesi. L'EDA viene eseguita calcolando statistiche di riepilogo e creando visualizzazioni di dati.

F

tabella dei fatti

Il tavolo centrale con [schema a stella](#). Memorizza dati quantitativi sulle operazioni aziendali. In genere, una tabella dei fatti contiene due tipi di colonne: quelle che contengono misure e quelle che contengono una chiave esterna per una tabella di dimensioni.

fallire velocemente

Una filosofia che utilizza test frequenti e incrementali per ridurre il ciclo di vita dello sviluppo. È una parte fondamentale di un approccio agile.

limite di isolamento dei guasti

Nel Cloud AWS, un limite come una zona di disponibilità Regione AWS, un piano di controllo o un piano dati che limita l'effetto di un errore e aiuta a migliorare la resilienza dei carichi di lavoro. Per ulteriori informazioni, consulta [AWS Fault Isolation Boundaries](#).

ramo di funzionalità

Vedi [filiale](#).

caratteristiche

I dati di input che usi per fare una previsione. Ad esempio, in un contesto di produzione, le caratteristiche potrebbero essere immagini acquisite periodicamente dalla linea di produzione.

importanza delle caratteristiche

Quanto è importante una caratteristica per le previsioni di un modello. Di solito viene espresso come punteggio numerico che può essere calcolato con varie tecniche, come Shapley Additive Explanations (SHAP) e gradienti integrati. Per ulteriori informazioni, consulta [Interpretabilità del modello di machine learning con AWS](#).

trasformazione delle funzionalità

Per ottimizzare i dati per il processo di machine learning, incluso l'arricchimento dei dati con fonti aggiuntive, il dimensionamento dei valori o l'estrazione di più set di informazioni da un singolo campo di dati. Ciò consente al modello di ML di trarre vantaggio dai dati. Ad esempio, se suddividi la data "2021-05-27 00:15:37" in "2021", "maggio", "giovedì" e "15", puoi aiutare l'algoritmo di apprendimento ad apprendere modelli sfumati associati a diversi componenti dei dati.

prompt con pochi scatti

Fornire a un [LLM](#) un numero limitato di esempi che dimostrino l'attività e il risultato desiderato prima di chiedergli di eseguire un'attività simile. Questa tecnica è un'applicazione dell'apprendimento contestuale, in cui i modelli imparano da esempi (immagini) incorporati nei prompt. Few-shot i suggerimenti possono essere efficaci per attività che richiedono una formattazione, un ragionamento o una conoscenza del dominio specifici. [Vedi anche zero-shot prompting](#).

FGAC

Vedi il controllo [granulare degli accessi](#).

controllo granulare degli accessi (FGAC)

L'uso di più condizioni per consentire o rifiutare una richiesta di accesso.

migrazione flash-cut

Un metodo di migrazione del database che utilizza la replica continua dei dati tramite [l'acquisizione dei dati delle modifiche](#) per migrare i dati nel più breve tempo possibile, anziché utilizzare un approccio graduale. L'obiettivo è ridurre al minimo i tempi di inattività.

FM

[Vedi il modello di base.](#)

modello di fondazione (FM)

Una grande rete neurale di deep learning che si è addestrata su enormi set di dati generalizzati e non etichettati. Le FM sono in grado di eseguire un'ampia varietà di attività generali, come comprendere il linguaggio, generare testo e immagini e conversare in linguaggio naturale. Per ulteriori informazioni, consulta [Cosa sono i modelli Foundation](#).

Gateway FM

[Un intermediario centralizzato che controlla e normalizza l'accesso ai modelli di base.](#) Conosciuto anche come gateway LLM.

G

IA generativa

Un sottoinsieme di modelli di [intelligenza artificiale](#) che sono stati addestrati su grandi quantità di dati e che possono utilizzare un semplice messaggio di testo per creare nuovi contenuti e artefatti, come immagini, video, testo e audio. Per ulteriori informazioni, consulta [Cos'è l'IA generativa](#).

blocco geografico

Vedi [restrizioni geografiche](#).

limitazioni geografiche (blocco geografico)

In Amazon CloudFront, un'opzione per impedire agli utenti di determinati paesi di accedere alle distribuzioni di contenuti. Puoi utilizzare un elenco consentito o un elenco di blocco per specificare

i paesi approvati e vietati. Per ulteriori informazioni, consulta [Limitare la distribuzione geografica dei contenuti](#) nella CloudFront documentazione.

Flusso di lavoro di GitFlow

Un approccio in cui gli ambienti inferiori e superiori utilizzano rami diversi in un repository di codice di origine. Il flusso di lavoro Gitflow è considerato obsoleto e il flusso di lavoro [basato su trunk è l'approccio moderno e preferito](#).

immagine dorata

Un'istantanea di un sistema o di un software che viene utilizzata come modello per distribuire nuove istanze di quel sistema o software. Ad esempio, nella produzione, un'immagine dorata può essere utilizzata per fornire software su più dispositivi e contribuire a migliorare la velocità, la scalabilità e la produttività nelle operazioni di produzione dei dispositivi.

strategia greenfield

L'assenza di infrastrutture esistenti in un nuovo ambiente. Quando si adotta una strategia greenfield per un'architettura di sistema, è possibile selezionare tutte le nuove tecnologie senza il vincolo della compatibilità con l'infrastruttura esistente, nota anche come [brownfield](#). Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

guardrail

Una regola di livello elevato che consente di governare risorse, policy e conformità tra le unità organizzative (OU). I guardrail preventivi applicano le policy per garantire l'allineamento agli standard di conformità. Vengono implementati utilizzando le policy di controllo dei servizi e i limiti delle autorizzazioni IAM. I guardrail di rilevamento rilevano le violazioni delle policy e i problemi di conformità e generano avvisi per porvi rimedio. Sono implementati utilizzando Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector e controlli personalizzati AWS Lambda .

guardrail (AI)

Meccanismi di sicurezza che filtrano, convalidano e limitano gli input e gli output degli [agenti](#) per contribuire a garantire un comportamento dell'IA responsabile e sicuro.

H

AH

Vedi [disponibilità elevata](#).

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. [AWS offre AWS SCT](#) che aiuta con le conversioni dello schema.

alta disponibilità (HA)

La capacità di un carico di lavoro di funzionare in modo continuo, senza intervento, in caso di sfide o disastri. I sistemi HA sono progettati per il failover automatico, fornire costantemente prestazioni di alta qualità e gestire carichi e guasti diversi con un impatto minimo sulle prestazioni.

modernizzazione storica

Un approccio utilizzato per modernizzare e aggiornare i sistemi di tecnologia operativa (OT) per soddisfare meglio le esigenze dell'industria manifatturiera. Uno storico è un tipo di database utilizzato per raccogliere e archiviare dati da varie fonti in una fabbrica.

dati di esclusione

[Una parte di dati storici etichettati che viene trattenuta da un set di dati utilizzata per addestrare un modello di apprendimento automatico.](#) È possibile utilizzare i dati di holdout per valutare le prestazioni del modello confrontando le previsioni del modello con i dati di holdout.

human-in-the-loop (HITL)

Un modello di flusso di lavoro in cui l'esecuzione degli [agenti](#) viene sospesa per la revisione e l'approvazione umana nei punti decisionali critici.

migrazione di database omogenea

Migrazione del database di origine in un database di destinazione che condivide lo stesso motore di database (ad esempio, da Microsoft SQL Server ad Amazon RDS per SQL Server). La migrazione omogenea fa in genere parte di un'operazione di rehosting o ridefinizione della piattaforma. Per migrare lo schema è possibile utilizzare le utilità native del database.

dati caldi

Dati a cui si accede frequentemente, ad esempio dati in tempo reale o dati di traduzione recenti. Questi dati richiedono in genere un livello o una classe di storage ad alte prestazioni per fornire risposte rapide alle query.

hotfix

Una soluzione urgente per un problema critico in un ambiente di produzione. A causa della sua urgenza, un hotfix viene in genere creato al di fuori del tipico DevOps flusso di lavoro di rilascio.

periodo di hypercare

Subito dopo la conversione, il periodo di tempo in cui un team di migrazione gestisce e monitora le applicazioni migrate nel cloud per risolvere eventuali problemi. In genere, questo periodo dura da 1 a 4 giorni. Al termine del periodo di hypercare, il team addetto alla migrazione in genere trasferisce la responsabilità delle applicazioni al team addetto alle operazioni cloud.

I

laC

Vedi [l'infrastruttura come codice](#).

Policy basata su identità

Una policy associata a uno o più principi IAM che definisce le relative autorizzazioni all'interno dell'Cloud AWS ambiente.

applicazione inattiva

Un'applicazione che prevede un uso di CPU e memoria medio compreso tra il 5% e il 20% in un periodo di 90 giorni. In un progetto di migrazione, è normale ritirare queste applicazioni o mantenerle on-premise.

IIoT

Vedi [Industrial Internet of Things](#).

infrastruttura immutabile

Un modello che implementa una nuova infrastruttura per i carichi di lavoro di produzione anziché aggiornare, applicare patch o modificare l'infrastruttura esistente. [Le infrastrutture immutabili sono intrinsecamente più coerenti, affidabili e prevedibili delle infrastrutture mutabili](#). Per ulteriori informazioni, consulta la best practice [Deploy using immutable](#) infrastructure nel Framework. AWS Well-Architected

VPC in ingresso (ingress)

In un'architettura AWS multi-account, un VPC che accetta, ispeziona e indirizza le connessioni di rete dall'esterno di un'applicazione. Nel documento [Architettura di riferimento per la sicurezza di](#)

[AWS](#) si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

Una strategia di conversione in cui si esegue la migrazione dell'applicazione in piccole parti anziché eseguire una conversione singola e completa. Ad esempio, inizialmente potresti spostare solo alcuni microservizi o utenti nel nuovo sistema. Dopo aver verificato che tutto funzioni correttamente, puoi spostare in modo incrementale microservizi o utenti aggiuntivi fino alla disattivazione del sistema legacy. Questa strategia riduce i rischi associati alle migrazioni di grandi dimensioni.

Industria 4.0

Un termine introdotto da [Klaus Schwab](#) nel 2016 per riferirsi alla modernizzazione dei processi di produzione attraverso progressi in termini di connettività, dati in tempo reale, automazione, analisi e. AI/ML

infrastruttura

Tutte le risorse e gli asset contenuti nell'ambiente di un'applicazione.

infrastruttura come codice (IaC)

Il processo di provisioning e gestione dell'infrastruttura di un'applicazione tramite un insieme di file di configurazione. Il processo IaC è progettato per aiutarti a centralizzare la gestione dell'infrastruttura, a standardizzare le risorse e a dimensionare rapidamente, in modo che i nuovi ambienti siano ripetibili, affidabili e coerenti.

Internet delle cose industriale (IIoT)

L'uso di sensori e dispositivi connessi a Internet nei settori industriali, come quello manifatturiero, energetico, automobilistico, sanitario, delle scienze della vita e dell'agricoltura. Per ulteriori informazioni, consulta [Creazione di una strategia di trasformazione digitale dell'Internet delle cose industriale \(IIoT\)](#).

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPC (uguali o diversi Regioni AWS), Internet e reti locali. Nel documento [Architettura di riferimento per la sicurezza di AWS](#) si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

Internet of Things (IoT)

La rete di oggetti fisici connessi con sensori o processori incorporati che comunicano con altri dispositivi e sistemi tramite Internet o una rete di comunicazione locale. Per ulteriori informazioni, consulta [Cos'è l'IoT?](#)

interpretabilità

Una caratteristica di un modello di machine learning che descrive il grado in cui un essere umano è in grado di comprendere in che modo le previsioni del modello dipendono dai suoi input. [Per ulteriori informazioni, consulta Interpretabilità del modello di machine learning con. AWS](#)

IoT

Vedi [Internet of Things](#).

libreria di informazioni IT (ITIL)

Una serie di best practice per offrire servizi IT e allinearli ai requisiti aziendali. ITIL fornisce le basi per ITSM.

gestione dei servizi IT (ITSM)

Attività associate alla progettazione, implementazione, gestione e supporto dei servizi IT per un'organizzazione. Per informazioni sull'integrazione delle operazioni cloud con gli strumenti ITSM, consulta la [guida all'integrazione delle operazioni](#).

ITIL

Vedi la [libreria di informazioni IT](#).

ITSM

Vedi [Gestione dei servizi IT](#).

L

controllo degli accessi basato su etichette (LBAC)

Un'implementazione del controllo di accesso obbligatorio (MAC) in cui agli utenti e ai dati stessi viene assegnato esplicitamente un valore di etichetta di sicurezza. L'intersezione tra l'etichetta di sicurezza utente e l'etichetta di sicurezza dei dati determina quali righe e colonne possono essere visualizzate dall'utente.

zona di destinazione

Una landing zone è un AWS ambiente multi-account ben progettato, scalabile e sicuro. Questo è un punto di partenza dal quale le organizzazioni possono avviare e distribuire rapidamente carichi di lavoro e applicazioni con fiducia nel loro ambiente di sicurezza e infrastruttura. Per ulteriori informazioni sulle zone di destinazione, consulta la sezione [Configurazione di un ambiente AWS multi-account sicuro e scalabile](#).

modello linguistico di grandi dimensioni (LLM)

Un modello di [intelligenza artificiale](#) di deep learning preaddestrato su una grande quantità di dati. Un LLM può svolgere più attività, come rispondere a domande, riepilogare documenti, tradurre testo in altre lingue e completare frasi. [Per ulteriori informazioni, consulta Cosa sono gli LLM](#).

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi [basato su etichette](#).

Privilegio minimo

La best practice di sicurezza per la concessione delle autorizzazioni minime richieste per eseguire un'attività. Per ulteriori informazioni, consulta [Applicazione delle autorizzazioni del privilegio minimo](#) nella documentazione di IAM.

eseguire il rehosting (lift and shift)

Vedi [7 R](#).

sistema little-endian

Un sistema che memorizza per primo il byte meno importante. Vedi anche [endianità](#).

LLM

Vedi modello [linguistico di grandi dimensioni](#).

ambienti inferiori

Vedi [ambiente](#).

M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione [Machine learning](#).

ramo principale

Vedi [filiale](#).

malware

Software progettato per compromettere la sicurezza o la privacy del computer. Il malware potrebbe interrompere i sistemi informatici, divulgare informazioni sensibili o ottenere accessi non autorizzati. Esempi di malware includono virus, worm, ransomware, trojan horse, spyware e keylogger.

servizi gestiti

Servizi AWS per cui AWS gestisce il livello di infrastruttura, il sistema operativo e le piattaforme e si accede agli endpoint per archiviare e recuperare i dati. Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e Amazon DynamoDB sono esempi di servizi gestiti. Questi sono noti anche come servizi astratti.

sistema di esecuzione della produzione (MES)

Un sistema software per tracciare, monitorare, documentare e controllare i processi di produzione che convertono le materie prime in prodotti finiti in officina.

MAP

Vedi [Migration Acceleration Program](#).

MCP

Vedi [Model Context Protocol](#).

Model Context Protocol (MCP)

[Un protocollo stateless per la comunicazione tra agenti e strumenti.](#)

Server MCP

Un servizio che espone uno o più [strumenti](#) tramite il [Model Context](#) Protocol.

meccanismo

Un processo completo in cui si crea uno strumento, si promuove l'adozione dello strumento e quindi si esaminano i risultati per apportare le modifiche. Un meccanismo è un ciclo che si rafforza e si migliora man mano che funziona. Per ulteriori informazioni, vedete [Creazione di meccanismi](#) nel AWS Well-Architected Framework.

account membro

Tutti gli account Account AWS diversi dall'account di gestione che fanno parte di un'organizzazione in AWS Organizations. Un account può essere membro di una sola organizzazione alla volta.

MEH

Vedi [sistema di esecuzione della produzione](#).

Message Queuing Telemetry Transport (MQTT)

[Un protocollo di comunicazione da macchina a macchina \(M2M\) leggero, basato sul publish/subscribe modello, per dispositivi IoT con risorse limitate.](#)

microservizio

Un piccolo servizio indipendente che comunica tramite API ben definite ed è in genere di proprietà di piccoli team autonomi. Ad esempio, un sistema assicurativo potrebbe includere microservizi che si riferiscono a funzionalità aziendali, come vendite o marketing, o sottodomini, come acquisti, reclami o analisi. I vantaggi dei microservizi includono agilità, dimensionamento flessibile, facilità di implementazione, codice riutilizzabile e resilienza. [Per ulteriori informazioni, consulta Integrazione dei microservizi utilizzando servizi serverless. AWS](#)

architettura di microservizi

Un approccio alla creazione di un'applicazione con componenti indipendenti che eseguono ogni processo applicativo come microservizio. Questi microservizi comunicano tramite un'interfaccia ben definita utilizzando API leggere. Ogni microservizio in questa architettura può essere aggiornato, distribuito e dimensionato per soddisfare la richiesta di funzioni specifiche di un'applicazione. Per ulteriori informazioni, vedere [Implementazione](#) dei microservizi su AWS.

Programma di accelerazione della migrazione (MAP)

Un AWS programma che fornisce consulenza, supporto, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per

eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

Il processo di trasferimento della maggior parte del portfolio di applicazioni sul cloud avviene a ondate, con più applicazioni trasferite a una velocità maggiore in ogni ondata. Questa fase utilizza le migliori pratiche e le lezioni apprese nelle fasi precedenti per implementare una fabbrica di migrazione di team, strumenti e processi per semplificare la migrazione dei carichi di lavoro attraverso l'automazione e la distribuzione agile. Questa è la terza fase della [strategia di migrazione AWS](#).

fabbrica di migrazione

Cross-functional team che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory includono in genere operazioni, analisti e proprietari aziendali, ingegneri addetti alla migrazione, sviluppatori e DevOps professionisti che lavorano nell'ambito degli sprint. Tra il 20% e il 50% di un portfolio di applicazioni aziendali è costituito da schemi ripetuti che possono essere ottimizzati con un approccio di fabbrica. Per ulteriori informazioni, consulta la [discussione sulle fabbriche di migrazione](#) e la [Guida alla fabbrica di migrazione al cloud](#) in questo set di contenuti.

metadati di migrazione

Le informazioni sull'applicazione e sul server necessarie per completare la migrazione. Ogni modello di migrazione richiede un set diverso di metadati di migrazione. Esempi di metadati di migrazione includono la sottorete, il gruppo di sicurezza e l'account di destinazione. AWS

modello di migrazione

Un'attività di migrazione ripetibile che descrive in dettaglio la strategia di migrazione, la destinazione della migrazione e l'applicazione o il servizio di migrazione utilizzati. Esempio: riorganizza la migrazione su Amazon EC2 AWS con Application Migration Service.

Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione a. Cloud AWS MPA offre una valutazione dettagliata del portfolio (dimensionamento corretto dei server, prezzi, confronto del TCO, analisi dei costi di migrazione) e pianificazione della migrazione (analisi e raccolta dei dati delle applicazioni, raggruppamento delle applicazioni, prioritizzazione delle migrazioni e pianificazione delle ondate). [Lo strumento MPA](#) (richiede l'accesso) è disponibile gratuitamente per tutti i AWS consulenti e i consulenti dei partner APN.

valutazione della preparazione alla migrazione (MRA)

Il processo di acquisizione di informazioni sullo stato di preparazione al cloud di un'organizzazione, l'identificazione dei punti di forza e di debolezza e la creazione di un piano d'azione per colmare le lacune identificate, utilizzando il CAF. AWS Per ulteriori informazioni, consulta la [guida di preparazione alla migrazione](#). MRA è la prima fase della [strategia di migrazione AWS](#).

strategia di migrazione

L'approccio utilizzato per migrare un carico di lavoro verso. Cloud AWS Per ulteriori informazioni, consulta la voce [7 R](#) in questo glossario e consulta [Mobilita la tua organizzazione per accelerare le migrazioni su larga scala](#).

ML

[Vedi machine learning](#).

modernizzazione

Trasformazione di un'applicazione obsoleta (legacy o monolitica) e della relativa infrastruttura in un sistema agile, elastico e altamente disponibile nel cloud per ridurre i costi, aumentare l'efficienza e sfruttare le innovazioni. Per ulteriori informazioni, vedere [Strategia per la modernizzazione delle applicazioni in](#). Cloud AWS

valutazione della preparazione alla modernizzazione

Una valutazione che aiuta a determinare la preparazione alla modernizzazione delle applicazioni di un'organizzazione, identifica vantaggi, rischi e dipendenze e determina in che misura l'organizzazione può supportare lo stato futuro di tali applicazioni. Il risultato della valutazione è uno schema dell'architettura di destinazione, una tabella di marcia che descrive in dettaglio le fasi di sviluppo e le tappe fondamentali del processo di modernizzazione e un piano d'azione per colmare le lacune identificate. Per ulteriori informazioni, vedere [Valutazione della preparazione alla modernizzazione per](#) le applicazioni in. Cloud AWS

applicazioni monolitiche (monoliti)

Applicazioni eseguite come un unico servizio con processi strettamente collegati. Le applicazioni monolitiche presentano diversi inconvenienti. Se una funzionalità dell'applicazione registra un picco di domanda, l'intera architettura deve essere dimensionata. L'aggiunta o il miglioramento delle funzionalità di un'applicazione monolitica diventa inoltre più complessa man mano che la base di codice cresce. Per risolvere questi problemi, puoi utilizzare un'architettura di microservizi. Per ulteriori informazioni, consulta la sezione [Scomposizione dei monoliti in microservizi](#).

MAPPA

Vedi [Migration Portfolio Assessment](#).

MQTT

Vedi [Message Queuing Telemetry Transport](#).

classificazione multiclasse

Un processo che aiuta a generare previsioni per più classi (prevedendo uno o più di due risultati). Ad esempio, un modello di machine learning potrebbe chiedere "Questo prodotto è un libro, un'auto o un telefono?" oppure "Quale categoria di prodotti è più interessante per questo cliente?"

infrastruttura mutabile

Un modello che aggiorna e modifica l'infrastruttura esistente per i carichi di lavoro di produzione. Per migliorare la coerenza, l'affidabilità e la prevedibilità, il AWS Well-Architected Framework consiglia l'uso di un'infrastruttura [immutabile](#) come best practice.

O

OAC

Vedi [Origin Access Control](#).

QUERCIA

Vedi [Origin Access Identity](#).

OCM

Vedi [gestione delle modifiche organizzative](#).

migrazione offline

Un metodo di migrazione in cui il carico di lavoro di origine viene eliminato durante il processo di migrazione. Questo metodo prevede tempi di inattività prolungati e viene in genere utilizzato per carichi di lavoro piccoli e non critici.

OI

Vedi [l'integrazione delle operazioni](#).

OLA

Vedi accordo a [livello operativo](#).

migrazione online

Un metodo di migrazione in cui il carico di lavoro di origine viene copiato sul sistema di destinazione senza essere messo offline. Le applicazioni connesse al carico di lavoro possono continuare a funzionare durante la migrazione. Questo metodo comporta tempi di inattività pari a zero o comunque minimi e viene in genere utilizzato per carichi di lavoro di produzione critici.

OPC-UA

Vedi [Open Process Communications - Unified Architecture](#).

Comunicazioni a processo aperto - Architettura unificata () OPC-UA

Un protocollo di comunicazione da macchina a macchina (M2M) per l'automazione industriale. OPC-UA fornisce uno standard di interoperabilità con schemi di crittografia, autenticazione e autorizzazione dei dati.

accordo a livello operativo (OLA)

Un accordo che chiarisce quali sono gli impegni reciproci tra i gruppi IT funzionali, a supporto di un accordo sul livello di servizio (SLA).

revisione della prontezza operativa (ORR)

Un elenco di domande e best practice associate che aiutano a comprendere, valutare, prevenire o ridurre la portata degli incidenti e dei possibili guasti. Per ulteriori informazioni, vedere [Operational Readiness Reviews \(ORR\)](#) nel Framework. AWS Well-Architected

tecnologia operativa (OT)

Sistemi hardware e software che interagiscono con l'ambiente fisico per controllare operazioni, apparecchiature e infrastrutture industriali. Nella produzione, l'integrazione di sistemi OT e di tecnologia dell'informazione (IT) è un obiettivo chiave per le trasformazioni [dell'Industria 4.0](#).

integrazione delle operazioni (OI)

Il processo di modernizzazione delle operazioni nel cloud, che prevede la pianificazione, l'automazione e l'integrazione della disponibilità. Per ulteriori informazioni, consulta la [guida all'integrazione delle operazioni](#).

trail organizzativo

Un percorso creato da noi AWS CloudTrail che registra tutti gli eventi di un'organizzazione per tutti Account AWS . AWS Organizations Questo percorso viene creato in ogni Account AWS che

fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, consulta [Creazione di un percorso per un'organizzazione](#) nella CloudTrail documentazione.

gestione del cambiamento organizzativo (OCM)

Un framework per la gestione di trasformazioni aziendali importanti e che comportano l'interruzione delle attività dal punto di vista delle persone, della cultura e della leadership. OCM aiuta le organizzazioni a prepararsi e passare a nuovi sistemi e strategie accelerando l'adozione del cambiamento, affrontando i problemi di transizione e promuovendo cambiamenti culturali e organizzativi. Nella strategia di AWS migrazione, questo framework si chiama accelerazione delle persone, a causa della velocità di cambiamento richiesta nei progetti di adozione del cloud. Per ulteriori informazioni, consultare la [Guida OCM](#).

controllo dell'accesso all'origine (OAC)

In CloudFront, un'opzione avanzata per limitare l'accesso per proteggere i contenuti di Amazon Simple Storage Service (Amazon S3). OAC supporta in tutto tutti i bucket S3 Regioni AWS, la crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche PUT e dirette al bucket S3. DELETE

identità di accesso origine (OAI)

Nel CloudFront, un'opzione per limitare l'accesso per proteggere i tuoi contenuti Amazon S3. Quando usi OAI, CloudFront crea un principale con cui Amazon S3 può autenticarsi. I principali autenticati possono accedere ai contenuti in un bucket S3 solo tramite una distribuzione specifica. CloudFront Vedi anche [OAC](#), che fornisce un controllo degli accessi più granulare e avanzato.

ORR

[Vedi la revisione della prontezza operativa.](#)

- NON

Vedi la [tecnologia operativa](#).

VPC in uscita (egress)

In un'architettura AWS multi-account, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. Nel documento [Architettura di riferimento per la sicurezza di AWS](#) si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

P

limite delle autorizzazioni

Una policy di gestione IAM collegata ai principali IAM per impostare le autorizzazioni massime che l'utente o il ruolo possono avere. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni](#) nella documentazione di IAM.

informazioni di identificazione personale (PII)

Informazioni che, se visualizzate direttamente o abbinate ad altri dati correlati, possono essere utilizzate per dedurre ragionevolmente l'identità di un individuo. Esempi di informazioni personali includono nomi, indirizzi e informazioni di contatto.

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le [informazioni di identificazione personale](#).

playbook

Una serie di passaggi predefiniti che raccolgono il lavoro associato alle migrazioni, come l'erogazione delle funzioni operative principali nel cloud. Un playbook può assumere la forma di script, runbook automatici o un riepilogo dei processi o dei passaggi necessari per gestire un ambiente modernizzato.

PLC

Vedi [controllore logico programmabile](#).

PLM

Vedi la gestione [del ciclo di vita del prodotto](#).

policy

[Un oggetto in grado di definire le autorizzazioni \(vedi politica basata sull'identità\), specificare le condizioni di accesso \(vedi politicabasata sulle risorse\) o definire le autorizzazioni massime per tutti gli account di un'organizzazione in \(vedi politica di controllo dei servizi\). AWS Organizations](#)

persistenza poliglotta

Scelta indipendente della tecnologia di archiviazione di dati di un microservizio in base ai modelli di accesso ai dati e ad altri requisiti. Se i microservizi utilizzano la stessa tecnologia di archiviazione di dati, possono incontrare problemi di implementazione o registrare prestazioni scadenti. I microservizi vengono implementati più facilmente e ottengono prestazioni e scalabilità migliori se utilizzano l'archivio dati più adatto alle loro esigenze.

valutazione del portfolio

Un processo di scoperta, analisi e definizione delle priorità del portfolio di applicazioni per pianificare la migrazione. Per ulteriori informazioni, consulta la pagina [Valutazione della preparazione alla migrazione](#).

predicate

Una condizione di interrogazione che restituisce o, in genere, si trova in una clausola `true`. `false`
`WHERE`

predicato pushdown

Una tecnica di ottimizzazione delle query del database che filtra i dati della query prima del trasferimento. Ciò riduce la quantità di dati che devono essere recuperati ed elaborati dal database relazionale e migliora le prestazioni delle query.

controllo preventivo

Un controllo di sicurezza progettato per impedire il verificarsi di un evento. Questi controlli sono la prima linea di difesa per impedire accessi non autorizzati o modifiche indesiderate alla rete. Per ulteriori informazioni, consulta [Controlli preventivi](#) in Implementazione dei controlli di sicurezza in AWS.

principale

Un'entità in AWS grado di eseguire azioni e accedere alle risorse. Questa entità è in genere un utente root per un Account AWS ruolo IAM o un utente. Per ulteriori informazioni, consulta Principali in [Termini e concetti dei ruoli](#) nella documentazione di IAM.

privacy fin dalla progettazione

Un approccio ingegneristico dei sistemi che tiene conto della privacy durante l'intero processo di sviluppo.

zone ospitate private

Un container che contiene informazioni su come si desidera che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più VPC. Per ulteriori informazioni, consulta [Utilizzo delle zone ospitate private](#) nella documentazione di Route 53.

controllo proattivo

Un [controllo di sicurezza](#) progettato per impedire l'implementazione di risorse non conformi. Questi controlli analizzano le risorse prima del loro provisioning. Se la risorsa non è conforme al

controllo, non viene fornita. Per ulteriori informazioni, consulta la [guida di riferimento sui controlli](#) nella AWS Control Tower documentazione e consulta Controlli [proattivi in Implementazione dei controlli](#) di sicurezza su AWS.

gestione del ciclo di vita del prodotto (PLM)

La gestione dei dati e dei processi di un prodotto durante l'intero ciclo di vita, dalla progettazione, sviluppo e lancio, attraverso la crescita e la maturità, fino al declino e alla rimozione.

Ambiente di produzione

[Vedi ambiente.](#)

controllore logico programmabile (PLC)

Nella produzione, un computer altamente affidabile e adattabile che monitora le macchine e automatizza i processi di produzione.

concatenamento rapido

Utilizzo dell'output di un prompt [LLM](#) come input per il prompt successivo per generare risposte migliori. Questa tecnica viene utilizzata per suddividere un'attività complessa in sottoattività o per perfezionare o espandere iterativamente una risposta preliminare. Aiuta a migliorare l'accuratezza e la pertinenza delle risposte di un modello e consente risultati più granulari e personalizzati.

pseudonimizzazione

Il processo di sostituzione degli identificatori personali in un set di dati con valori segnaposto. La pseudonimizzazione può aiutare a proteggere la privacy personale. I dati pseudonimizzati sono ancora considerati dati personali.

publish/subscribe (pub/sub)

Un modello che consente comunicazioni asincrone tra microservizi per migliorare la scalabilità e la reattività. Ad esempio, in un [MES](#) basato su microservizi, un microservizio può pubblicare messaggi di eventi su un canale a cui altri microservizi possono abbonarsi. Il sistema può aggiungere nuovi microservizi senza modificare il servizio di pubblicazione.

Q

Piano di query

Una serie di passaggi, come le istruzioni, utilizzati per accedere ai dati in un sistema di database relazionale SQL.

regressione del piano di query

Quando un ottimizzatore del servizio di database sceglie un piano non ottimale rispetto a prima di una determinata modifica all'ambiente di database. Questo può essere causato da modifiche a statistiche, vincoli, impostazioni dell'ambiente, associazioni dei parametri di query e aggiornamenti al motore di database.

R

Matrice RACI

Vedi [responsabile, responsabile, consultato, informato \(RACI\)](#).

RAG

Vedi [Retrieval](#) Augmented Generation.

ransomware

Un software dannoso progettato per bloccare l'accesso a un sistema informatico o ai dati fino a quando non viene effettuato un pagamento.

Matrice RASCI

Vedi [responsabile, responsabile, consultato, informato \(RACI\)](#).

RCAC

Vedi controllo dell'[accesso a righe e colonne](#).

replica di lettura

Una copia di un database utilizzata per scopi di sola lettura. È possibile indirizzare le query alla replica di lettura per ridurre il carico sul database principale.

riprogettare

Vedi [7 Rs](#).

obiettivo del punto di ripristino (RPO)

Il periodo di tempo massimo accettabile dall'ultimo punto di ripristino dei dati. Questo determina ciò che si considera una perdita di dati accettabile tra l'ultimo punto di ripristino e l'interruzione del servizio.

obiettivo del tempo di ripristino (RTO)

Il ritardo massimo accettabile tra l'interruzione del servizio e il ripristino del servizio.

rifattorizzare

Vedi [7 R.](#)

Region

Una raccolta di AWS risorse in un'area geografica. Ciascuna Regione AWS è isolata e indipendente dalle altre per fornire tolleranza agli errori, stabilità e resilienza. Per ulteriori informazioni, consulta [Specificare cosa può usare Regioni AWS il tuo account.](#)

regressione

Una tecnica di ML che prevede un valore numerico. Ad esempio, per risolvere il problema "A che prezzo verrà venduta questa casa?" un modello di ML potrebbe utilizzare un modello di regressione lineare per prevedere il prezzo di vendita di una casa sulla base di dati noti sulla casa (ad esempio, la metratura).

riospitare

Vedi [7 R.](#)

rilascio

In un processo di implementazione, l'atto di promuovere modifiche a un ambiente di produzione.

trasferisco

Vedi [7 Rs.](#)

ripiattaforma

Vedi [7 Rs.](#)

riacquisto

Vedi [7 Rs.](#)

resilienza

La capacità di un'applicazione di resistere o ripristinare le interruzioni. [L'elevata disponibilità e il disaster recovery](#) sono considerazioni comuni quando si pianifica la resilienza in Cloud AWS. [Per ulteriori informazioni, vedere Cloud AWS Resilience.](#)

policy basata su risorse

Una policy associata a una risorsa, ad esempio un bucket Amazon S3, un endpoint o una chiave di crittografia. Questo tipo di policy specifica a quali principali è consentito l'accesso, le azioni supportate e qualsiasi altra condizione che deve essere soddisfatta.

matrice di assegnazione di responsabilità (RACI)

Una matrice che definisce i ruoli e le responsabilità di tutte le parti coinvolte nelle attività di migrazione e nelle operazioni cloud. Il nome della matrice deriva dai tipi di responsabilità definiti nella matrice: responsabile (R), responsabile (A), consultato (C) e informato (I). Il tipo di supporto (S) è facoltativo. Se includi il supporto, la matrice viene chiamata matrice RASCI e, se la escludi, viene chiamata matrice RACI.

controllo reattivo

Un controllo di sicurezza progettato per favorire la correzione di eventi avversi o deviazioni dalla baseline di sicurezza. Per ulteriori informazioni, consulta [Controlli reattivi](#) in Implementazione dei controlli di sicurezza in AWS.

retain

Vedi [7 R](#).

andare in pensione

Vedi [7 Rs](#).

Retrieval Augmented Generation (RAG)

Una tecnologia di [intelligenza artificiale generativa](#) in cui un [LLM](#) fa riferimento a una fonte di dati autorevole esterna alle sue fonti di dati di formazione prima di generare una risposta. Ad esempio, un modello RAG potrebbe eseguire una ricerca semantica nella knowledge base o nei dati personalizzati di un'organizzazione. Per ulteriori informazioni, consulta [Cos'è il RAG](#).

rotazione

Processo di aggiornamento periodico di un [segreto](#) per rendere più difficile l'accesso alle credenziali da parte di un utente malintenzionato.

controllo dell'accesso a righe e colonne (RCAC)

L'uso di espressioni SQL di base e flessibili con regole di accesso definite. RCAC è costituito da autorizzazioni di riga e maschere di colonna.

RPO

Vedi [obiettivo del punto di ripristino](#).

VERSO

Vedi [obiettivo del tempo di ripristino](#).

runbook

Un insieme di procedure manuali o automatizzate necessarie per eseguire un'attività specifica. In genere sono progettati per semplificare operazioni o procedure ripetitive con tassi di errore elevati.

S

SAML 2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità abilita il single sign-on (SSO) federato, in modo che gli utenti possano accedere Console di gestione AWS o chiamare le operazioni AWS API senza che tu debba creare un utente in IAM per tutti i membri dell'organizzazione. Per ulteriori informazioni sulla federazione basata su SAML 2.0, consulta [Informazioni sulla federazione basata su SAML 2.0](#) nella documentazione di IAM.

SCADA

Vedi [controllo di supervisione e acquisizione dati](#).

SCP

Vedi la [politica di controllo del servizio](#).

Secret

In Gestione dei segreti AWS, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, consulta [Cosa c'è in un segreto di Secrets Manager?](#) nella documentazione di Secrets Manager.

sicurezza fin dalla progettazione

Un approccio di ingegneria dei sistemi che tiene conto della sicurezza durante l'intero processo di sviluppo.

controllo di sicurezza

Un guardrail tecnico o amministrativo che impedisce, rileva o riduce la capacità di un autore di minacce di sfruttare una vulnerabilità di sicurezza. [Esistono quattro tipi principali di controlli di sicurezza: preventivi, investigativi, reattivi e proattivi.](#)

rafforzamento della sicurezza

Il processo di riduzione della superficie di attacco per renderla più resistente agli attacchi. Può includere azioni come la rimozione di risorse che non sono più necessarie, l'implementazione di best practice di sicurezza che prevedono la concessione del privilegio minimo o la disattivazione di funzionalità non necessarie nei file di configurazione.

sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM)

Strumenti e servizi che combinano sistemi di gestione delle informazioni di sicurezza (SIM) e sistemi di gestione degli eventi di sicurezza (SEM). Un sistema SIEM raccoglie, monitora e analizza i dati da server, reti, dispositivi e altre fonti per rilevare minacce e violazioni della sicurezza e generare avvisi.

automazione della risposta alla sicurezza

Un'azione predefinita e programmata progettata per rispondere o porre rimedio automaticamente a un evento di sicurezza. Queste automazioni fungono da controlli di sicurezza [investigativi](#) o [reattivi](#) che aiutano a implementare le migliori pratiche di sicurezza. AWS Esempi di azioni di risposta automatizzate includono la modifica di un gruppo di sicurezza VPC, l'applicazione di patch a un'istanza Amazon EC2 o la rotazione delle credenziali.

Crittografia lato server

Crittografia dei dati a destinazione, da parte di chi li riceve. Servizio AWS

Policy di controllo dei servizi (SCP)

Una policy che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in AWS Organizations. Le SCP definiscono i guardrail o fissano i limiti alle azioni che un amministratore può delegare a utenti o ruoli. Puoi utilizzare le SCP come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta [le politiche di controllo del servizio](#) nella AWS Organizations documentazione.

endpoint del servizio

L'URL del punto di ingresso per un Servizio AWS. Puoi utilizzare l'endpoint per connetterti a livello di programmazione al servizio di destinazione. Per ulteriori informazioni, consulta [Endpoint del Servizio AWS](#) nei Riferimenti generali di AWS.

accordo sul livello di servizio (SLA)

Un accordo che chiarisce ciò che un team IT promette di offrire ai propri clienti, ad esempio l'operatività e le prestazioni del servizio.

indicatore del livello di servizio (SLI)

Misurazione di un aspetto prestazionale di un servizio, ad esempio il tasso di errore, la disponibilità o la velocità effettiva.

obiettivo a livello di servizio (SLO)

[Una metrica target che rappresenta lo stato di un servizio, misurato da un indicatore del livello di servizio.](#)

Modello di responsabilità condivisa

Un modello che descrive la responsabilità condivisa AWS per la sicurezza e la conformità del cloud. AWS è responsabile della sicurezza del cloud, mentre tu sei responsabile della sicurezza nel cloud. Per ulteriori informazioni, consulta [Modello di responsabilità condivisa](#).

Shadow AI

Applicazioni di [intelligenza artificiale](#) non autorizzate create o utilizzate al di fuori dei canali regolamentati all'interno di un'organizzazione.

SIEM

Vedi il [sistema di gestione delle informazioni e degli eventi sulla sicurezza](#).

punto di errore singolo (SPOF)

Un guasto in un singolo componente critico di un'applicazione che può disturbare il sistema.

SLAM

Vedi il contratto sul [livello di servizio](#).

SLI

Vedi l'indicatore del [livello di servizio](#).

LENTA

Vedi obiettivo del [livello di servizio](#).

modello split-and-seed

Un modello per dimensionare e accelerare i progetti di modernizzazione. Man mano che vengono definite nuove funzionalità e versioni dei prodotti, il team principale si divide per creare nuovi team di prodotto. Questo aiuta a dimensionare le capacità e i servizi dell'organizzazione, migliora la produttività degli sviluppatori e supporta una rapida innovazione. Per ulteriori informazioni, vedere [Approccio graduale alla modernizzazione delle applicazioni in](#). Cloud AWS

SPOF

Vedi [punto di errore singolo](#).

schema a stella

Una struttura organizzativa di database che utilizza un'unica tabella dei fatti di grandi dimensioni per archiviare i dati transazionali o misurati e utilizza una o più tabelle dimensionali più piccole per memorizzare gli attributi dei dati. Questa struttura è progettata per l'uso in un [data warehouse](#) o per scopi di business intelligence.

modello del fico strangolatore

Un approccio alla modernizzazione dei sistemi monolitici mediante la riscrittura e la sostituzione incrementali delle funzionalità del sistema fino alla disattivazione del sistema legacy. Questo modello utilizza l'analogia di una pianta di fico che cresce fino a diventare un albero robusto e alla fine annienta e sostituisce il suo ospite. Il modello è stato [introdotto da Martin Fowler](#) come metodo per gestire il rischio durante la riscrittura di sistemi monolitici. Per un esempio di come applicare questo modello, consulta [Modernizzare i servizi Web Microsoft ASP.NET \(ASMX\) legacy in modo incrementale utilizzando contenitori e Amazon API Gateway](#).

sottorete

Un intervallo di indirizzi IP nel VPC. Una sottorete deve risiedere in una singola zona di disponibilità.

controllo di supervisione e acquisizione dati (SCADA)

Nella produzione, un sistema che utilizza hardware e software per monitorare gli asset fisici e le operazioni di produzione.

crittografia simmetrica

Un algoritmo di crittografia che utilizza la stessa chiave per crittografare e decrittografare i dati.

test sintetici

Test di un sistema in modo da simulare le interazioni degli utenti per rilevare potenziali problemi o monitorare le prestazioni. Puoi usare [Amazon CloudWatch Synthetics](#) per creare questi test.

prompt di sistema

Una tecnica per fornire contesto, istruzioni o linee guida a un [LLM](#) per indirizzarne il comportamento. I prompt di sistema aiutano a impostare il contesto e stabilire regole per le interazioni con gli utenti.

T

tag

Key-value coppie che fungono da metadati per l'organizzazione delle risorse. AWS Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse. Per ulteriori informazioni, consulta [Tagging delle risorse AWS](#).

variabile di destinazione

Il valore che stai cercando di prevedere nel machine learning supervisionato. Questo è indicato anche come variabile di risultato. Ad esempio, in un ambiente di produzione la variabile di destinazione potrebbe essere un difetto del prodotto.

elenco di attività

Uno strumento che viene utilizzato per tenere traccia dei progressi tramite un runbook. Un elenco di attività contiene una panoramica del runbook e un elenco di attività generali da completare. Per ogni attività generale, include la quantità stimata di tempo richiesta, il proprietario e lo stato di avanzamento.

ambiente di test

Vedi [ambiente](#).

training

Fornire dati da cui trarre ispirazione dal modello di machine learning. I dati di training devono contenere la risposta corretta. L'algoritmo di apprendimento trova nei dati di addestramento i pattern che mappano gli attributi dei dati di input al target (la risposta che si desidera prevedere). Produce un modello di ML che acquisisce questi modelli. Puoi quindi utilizzare il modello di ML per creare previsioni su nuovi dati di cui non si conosce il target.

strumento

Una funzione o API che un [agente](#) può richiamare per eseguire operazioni in sistemi esterni.

Transit Gateway

Un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti on-premise. Per ulteriori informazioni, consulta [Cos'è un gateway di transito](#) nella AWS Transit Gateway documentazione.

flusso di lavoro basato su trunk

Un approccio in cui gli sviluppatori creano e testano le funzionalità localmente in un ramo di funzionalità e quindi uniscono tali modifiche al ramo principale. Il ramo principale viene quindi integrato negli ambienti di sviluppo, preproduzione e produzione, in sequenza.

Accesso attendibile

Concessione delle autorizzazioni a un servizio specificato dall'utente per eseguire attività all'interno dell'organizzazione AWS Organizations e nei suoi account per conto dell'utente. Il servizio attendibile crea un ruolo collegato al servizio in ogni account, quando tale ruolo è necessario, per eseguire attività di gestione per conto dell'utente. Per ulteriori informazioni, consulta [Utilizzo AWS Organizations con altri AWS servizi](#) nella AWS Organizations documentazione.

regolazione

Modificare alcuni aspetti del processo di training per migliorare la precisione del modello di ML. Ad esempio, puoi addestrare il modello di ML generando un set di etichette, aggiungendo etichette e quindi ripetendo questi passaggi più volte con impostazioni diverse per ottimizzare il modello.

team da due pizze

Una piccola DevOps squadra che puoi sfamare con due pizze. Un team composto da due persone garantisce la migliore opportunità possibile di collaborazione nello sviluppo del software.

U

incertezza

Un concetto che si riferisce a informazioni imprecise, incomplete o sconosciute che possono minare l'affidabilità dei modelli di machine learning predittivi. Esistono due tipi di incertezza:

l'incertezza epistemica, che è causata da dati limitati e incompleti, mentre l'incertezza aleatoria è causata dal rumore e dalla casualità insiti nei dati.

compiti indifferenziati

Conosciuto anche come sollevamento di carichi pesanti, è un lavoro necessario per creare e far funzionare un'applicazione, ma che non apporta valore diretto all'utente finale né offre vantaggi competitivi. Esempi di attività indifferenziate includono l'approvvigionamento, la manutenzione e la pianificazione della capacità.

ambienti superiori

[Vedi ambiente.](#)

V

vacuum

Un'operazione di manutenzione del database che prevede la pulizia dopo aggiornamenti incrementali per recuperare lo spazio di archiviazione e migliorare le prestazioni.

controllo delle versioni

Processi e strumenti che tengono traccia delle modifiche, ad esempio le modifiche al codice di origine in un repository.

Peering VPC

Una connessione tra due VPC che consente di instradare il traffico tramite indirizzi IP privati. Per ulteriori informazioni, consulta [Che cos'è il peering VPC?](#) nella documentazione di Amazon VPC.

vulnerabilità

Un difetto software o hardware che compromette la sicurezza del sistema.

W

cache calda

Una cache del buffer che contiene dati correnti e pertinenti a cui si accede frequentemente. L'istanza di database può leggere dalla cache del buffer, il che richiede meno tempo rispetto alla lettura dalla memoria dal disco principale.

dati caldi

Dati a cui si accede raramente. Quando si eseguono interrogazioni di questo tipo di dati, in genere sono accettabili interrogazioni moderatamente lente.

funzione finestra

Una funzione SQL che esegue un calcolo su un gruppo di righe che si riferiscono in qualche modo al record corrente. Le funzioni della finestra sono utili per l'elaborazione di attività, come il calcolo di una media mobile o l'accesso al valore delle righe in base alla posizione relativa della riga corrente.

Carico di lavoro

Una raccolta di risorse e codice che fornisce valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo back-end.

flusso di lavoro

Gruppi funzionali in un progetto di migrazione responsabili di una serie specifica di attività. Ogni flusso di lavoro è indipendente ma supporta gli altri flussi di lavoro del progetto. Ad esempio, il flusso di lavoro del portfolio è responsabile della definizione delle priorità delle applicazioni, della pianificazione delle ondate e della raccolta dei metadati di migrazione. Il flusso di lavoro del portfolio fornisce queste risorse al flusso di lavoro di migrazione, che quindi migra i server e le applicazioni.

VERME

Vedi [scrivere una volta, leggere molti](#).

WQF

Vedi [AWS Workload Qualification Framework](#).

scrivi una volta, leggi molte (WORM)

Un modello di storage che scrive i dati una sola volta e ne impedisce l'eliminazione o la modifica. Gli utenti autorizzati possono leggere i dati tutte le volte che è necessario, ma non possono modificarli. Questa infrastruttura di archiviazione dei dati è considerata [immutabile](#).

Z

exploit zero-day

[Un attacco, in genere malware, che sfrutta una vulnerabilità zero-day.](#)

vulnerabilità zero-day

Un difetto o una vulnerabilità assoluta in un sistema di produzione. Gli autori delle minacce possono utilizzare questo tipo di vulnerabilità per attaccare il sistema. Gli sviluppatori vengono spesso a conoscenza della vulnerabilità causata dall'attacco.

prompt zero-shot

Fornire a un [LLM](#) le istruzioni per eseguire un'attività ma non esempi (immagini) che possano aiutarla. Il LLM deve utilizzare le sue conoscenze pre-addestrate per gestire l'attività. L'efficacia del prompt zero-shot dipende dalla complessità dell'attività e dalla qualità del prompt. [Vedi anche few-shot prompting.](#)

applicazione zombie

Un'applicazione che prevede un utilizzo CPU e memoria inferiore al 5%. In un progetto di migrazione, è normale ritirare queste applicazioni.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.