Creazione di una strategia per il cloud singolo, ibrido e multicloud nell'istruzione

AWS Guida prescrittiva

AWS Guida prescrittiva: Creazione di una strategia per il cloud singolo, ibrido e multicloud nell'istruzione

Table of Contents

Creazione di una strategia per il cloud singolo, ibrido e multicloud nell'istruzione

Amazon Web Services (collaboratori)

Settembre 2023 (cronologia del documento)

Gli istituti di istruzione stanno cercando di supportare funzioni come l'apprendimento remoto, la ricerca, l'esperienza degli studenti, l'analisi dei dati e l'amministrazione con l'agilità, i risparmi sui costi, la sicurezza e la resilienza offerti dal cloud computing. Molte organizzazioni stanno valutando le implementazioni ibride e multicloud come parte di questa trasformazione digitale.

Questo paper fornisce linee guida prescrittive sulla creazione di una tecnologia e di una strategia di governance singola, ibrida e multicloud, per i dirigenti e i responsabili delle decisioni degli istituti scolastici che stanno valutando le loro opzioni cloud. Questa guida si basa sulla nostra esperienza di AWS collaborazione con oltre 14.000 istituti di istruzione di tutte le dimensioni in tutto il mondo, dalle scuole primarie e secondarie all'istruzione superiore.

Panoramica di

Man mano che gli istituti di istruzione si trasformano digitalmente per offrire servizi ed esperienze differenziati a studenti, genitori, docenti, personale e comunità, devono affrontare una moltitudine di decisioni tecniche. Molte organizzazioni hanno già deciso di adottare il cloud per aumentare l'agilità, l'elasticità, la resilienza, la sicurezza e il risparmio sui costi. Sulla base delle relazioni e degli investimenti esistenti tra i vari team, la maggior parte delle organizzazioni utilizza una combinazione di data center locali, strutture di colocation e provider di cloud. Data la disponibilità di diverse opzioni cloud, gli istituti scolastici devono spesso scegliere tra modelli di implementazione singoli, ibridi e multicloud (definiti nella sezione Strategie di implementazione del cloud).

Il multicloud, ovvero l'uso di servizi di almeno due provider di servizi cloud, non è raro oggi per molti istituti. Il tuo team IT potrebbe preferire un provider di servizi cloud, mentre altri gruppi, reparti o singoli utenti potrebbero scegliere o utilizzare già provider alternativi. Gli istituti di istruzione che non dispongono di una strategia chiara che li guidi verso il modello di implementazione cloud appropriato devono affrontare molte sfide. Queste includono complessità non necessarie, aumento della domanda di personale, governance incoerente e approcci con il minimo comune denominatore che le limitano al sottoinsieme di funzionalità di base comuni a tutti i provider. Ogni sfida soffoca l'innovazione e rallenta la trasformazione digitale.

Al contrario, se disponi di una strategia cloud che ti guida all'uso del cloud singolo, ibrido e multicloud, puoi soddisfare i requisiti della tua missione educativa sfruttando al contempo i vantaggi del cloud in un modo che sia operativamente sostenibile per il successo a lungo termine. Per creare questa strategia, consigliamo quanto segue:

- Seleziona un provider cloud primario e strategico.
- Stabilisci un Cloud Center of Excellence (CCoE).
- Distingui tra applicazioni SaaS (Software as a Service) e servizi cloud di base.
- Stabilisci i requisiti di sicurezza e governance per ogni provider di servizi cloud.
- Adotta soluzioni gestite native per il cloud laddove possibile e pratico.
- Implementa architetture ibride laddove esistenti, gli investimenti locali incentivano l'uso continuato.
- Riserva il multicloud solo per i carichi di lavoro che non sono in grado di soddisfare i requisiti tecnici o aziendali tramite un unico provider di cloud.

Queste best practice sono illustrate in dettaglio nella sezione Consigli di questo paper. Ogni raccomandazione è importante, ma le priorità del tuo istituto dipenderanno dalla fase di adozione del cloud. Ad esempio, se hai appena iniziato ad adottare il cloud, concentrati sulla selezione di un provider cloud strategico primario, sulla creazione di una CCo E e sull'adozione di soluzioni gestite native per il cloud. Se utilizzi già un unico provider di servizi cloud, concentrati sulla definizione dei requisiti di sicurezza e governance di base e prendi in considerazione le architetture ibride quando gli investimenti esistenti nei data center incentivano l'uso continuato. Se la tua organizzazione utilizza già più provider di servizi cloud, concentrati sulla differenziazione delle applicazioni SaaS e sulla prenotazione delle implementazioni multicloud a quei rari carichi di lavoro che lo richiedono realmente.

Indice

Strategie di implementazione del cloud

AWS definisce il cloud computing come la fornitura su richiesta di risorse IT su Internet con prezzi. pay-as-you-go Invece di acquistare, possedere e mantenere centri dati e server fisici, è possibile accedere a servizi tecnologici, come potenza di calcolo, archiviazione e database, in base alle necessità da un provider di servizi cloud. Il cloud computing consente agli istituti scolastici di evitare oneri indifferenziati come l'approvvigionamento di hardware, la manutenzione e la pianificazione della capacità. Quando adotti e distribuisci soluzioni cloud, puoi scegliere tra diversi modelli: cloud singolo, cloud ibrido e multicloud.

Cloud singolo

Questo modello utilizza un solo fornitore di servizi cloud. Le applicazioni e i carichi di lavoro a cloud singolo potrebbero essere implementati direttamente nel cloud o precedentemente ospitati in un altro ambiente e migrati nel cloud. Questi carichi di lavoro potrebbero utilizzare servizi di infrastruttura di livello inferiore forniti dal proprio provider di cloud o sfruttare anche servizi gestiti di livello superiore. Indipendentemente da ciò, questo modello adotta un unico provider cloud e utilizza solo i servizi cloud di quel provider.

Cloud ibrido

Un modello di cloud ibrido distribuisce le risorse tra il data center locale dell'organizzazione e almeno un provider di servizi cloud. In genere, lo scopo di questo modello è estendere l'infrastruttura di un'organizzazione nel cloud mantenendo al contempo la connettività privata con i sistemi interni esistenti che risiedono in sede.

Multicloud

Un modello multicloud distribuisce le risorse tra e utilizza i servizi di almeno due provider di servizi cloud. Un'organizzazione potrebbe scegliere di essere multicloud, ma più spesso questo è il risultato involontario del fatto che singoli team, reparti o membri del personale hanno le proprie preferenze per i diversi provider di cloud.

Raccomandazioni

Ora che hai una conoscenza di base del cloud singolo, del cloud ibrido e del multicloud, questa sezione fornisce consigli dettagliati per la scelta di un modello.

- Seleziona un provider cloud primario e strategico
- Stabilisci una CCo E
- Distinguere tra applicazioni SaaS e servizi cloud di base
- Stabilisci i requisiti di sicurezza e governance per ogni provider di servizi cloud
- Adotta servizi gestiti nativi del cloud laddove possibile e pratico
- Implementa architetture ibride laddove esistenti, gli investimenti locali incentivano l'uso continuato
- Riserva il multicloud solo ai carichi di lavoro che non sono in grado di soddisfare i requisiti tecnici o aziendali tramite un unico provider di cloud

Seleziona un provider cloud primario e strategico

L'adozione del cloud offre una vasta gamma di vantaggi essenziali per la modernizzazione dell'IT, l'economicità e l'innovazione. Tuttavia, l'adozione di tecnologie cloud oltre alle applicazioni SaaS limitate può introdurre sfide che gli istituti scolastici devono pianificare attentamente per evitare costi e complessità inutili. I cambiamenti tecnologici e aziendali legati all'implementazione dei carichi di lavoro nel cloud richiedono l'abilitazione del personale e l'adeguamento dell'infrastruttura di base, tra cui networking, sicurezza, governance e operazioni.

L'approccio migliore per affrontare queste sfide in modo efficace, soprattutto se l'organizzazione è nelle prime fasi del suo percorso verso il cloud, è selezionare un provider cloud primario e strategico per supportare la maggior parte dei carichi di lavoro. Inizia con un'adozione mirata incentrata su quel provider in modo da semplificare e accelerare la realizzazione dei vantaggi del cloud. La selezione di un provider cloud primario non è una decisione esclusiva e irreversibile. Consente all'organizzazione di far evolvere l'adozione del cloud in modo iterativo. Puoi iniziare concentrandoti su alcuni servizi e poi espanderti ad altri servizi cloud se e dove necessario, senza ritardare i vantaggi complessivi del cloud. Questo approccio massimizza la capacità dell'organizzazione di sfruttare le capacità di un provider, concentrare e sviluppare le competenze dei dipendenti e le relazioni con i partner terzi e semplificare la gestione dei fornitori.

Abbiamo visto clienti intraprendere il loro percorso verso il cloud cercando di adottare contemporaneamente più provider di servizi cloud, ma in seguito si sono pentiti di quella decisione e della complessità che ha introdotto. Gartner condivide queste informazioni nel suo articolo, 6 passaggi per la pianificazione di una strategia cloud, in cui la fase 2 è «Dare priorità a un provider primario in architetture multicloud».

Ogni provider di servizi cloud introduce diversi modelli operativi e di supporto, gestione delle identità e degli accessi, reti, operazioni, funzionalità di conformità e altro ancora. È meglio padroneggiare il modello operativo di un provider di servizi cloud alla volta.È quindi possibile incorporare servizi cloud aggiuntivi in modo iterativo e incrementale, laddove razionalizzato. Molti fattori possono influenzare la tua decisione di adottare un provider di cloud primario, ma utilizza le seguenti domande chiave per guidare la tua scelta.

- Quale ampiezza e profondità di servizi offre il provider?

  Diversi provider di servizi cloud offrono servizi diversi. Come minimo, assicurati che il tuo provider principale disponga delle capacità necessarie per supportare tutti i tuoi requisiti funzionali e le tue esigenze operative trasversali come sicurezza, governance e automazione. Scegliete un fornitore che offra queste funzionalità con una comprovata esperienza di innovazione ed eccellenza operativa. Considerate non solo le vostre applicazioni, ma anche i vostri dati. Pensa ai futuri modelli di integrazione e trasferimento dei dati per limitare il costo, la latenza e la complessità dello spostamento di grandi quantità di dati tra i provider. Scegliete un provider che offra la più ampia gamma e profondità possibile di servizi per soddisfare le vostre attuali esigenze in materia di applicazioni e dati e anche per sbloccare nuovi casi d'uso in grado di soddisfare le esigenze del vostro istituto man mano che cambiano nel tempo.
- Il provider è in grado di supportare tutte le vostre esigenze di sicurezza e conformità?

  Nell'istruzione, la sicurezza e la conformità sono fondamentali per qualsiasi implementazione tecnologica. Scegli un provider di servizi cloud in grado di soddisfare tutte le tue esigenze di sicurezza e conformità. Strumenti come questi AWS Artifactpossono aiutarti a valutare i provider offrendo una risorsa centrale per l'accesso su richiesta ai report di sicurezza e conformità. Considerate non solo la sicurezza e la conformità dell'infrastruttura e dei servizi del provider di servizi cloud, ma anche quanto sia facile per voi progettare soluzioni sicure e conformi utilizzando tali servizi. Preferisci un provider che offra una combinazione di soluzioni predefinite, avvio rapido e linee guida prescrittive per accelerare l'adozione sicura del cloud.
- Il provider dispone di una solida rete di partner?

Nessuna organizzazione si sottopone da sola alla trasformazione del cloud. Per accelerare l'adozione, è necessario utilizzare i servizi e le competenze del provider di servizi cloud e la sua rete di partner. Questa rete include partner tecnologici che forniscono software che funziona, si integra o supporta la tecnologia cloud, nonché partner di consulenza che possono aiutarti a progettare, creare, eseguire e gestire le tue applicazioni nel cloud. Scoprirai che molti fornitori di tecnologia didattica, fornitori di software indipendenti (ISVs), consulenti e rivenditori con cui già lavori fanno parte della rete di partner del provider di servizi cloud. Preferisci un provider di servizi cloud che disponga della rete più solida di partner con competenze verificate. Avere partner con comprovate competenze tecniche e di settore è fondamentale.

- Che tipo di supporto e abilitazione offre il provider?

  Per adottare con successo qualsiasi nuova tecnologia, sono necessari meccanismi per richiedere formazione e assistenza, tra cui raccomandazioni sulle migliori pratiche, linee guida alla configurazione e risoluzione dei problemi. La scelta di un provider di servizi cloud che offra solide opzioni di supporto e formazione ti preparerà al successo. Esplora il modello e le risorse di supporto ufficiali del provider, nonché tutte le risorse disponibili di terze parti o basate sulla community, come blog, forum, video e guide pratiche. Prendi in considerazione non solo i programmi di supporto tecnico del fornitore, ma anche i programmi incentrati sulla trasformazione aziendale e culturale. Ad esempio, il AWS Cloud Adoption Framework (AWS CAF) aiuta le organizzazioni a trasformarsi digitalmente concentrandosi su prospettive che includono i processi aziendali e le persone, non solo la tecnologia. Preferisci un provider di servizi cloud che offra ampie opzioni di formazione e una community e un modello di supporto collaudati e affidabili.

Stabilisci una CCo E

Prendi in considerazione l'idea di far evolvere la tua funzione di leadership nel cloud attraverso un ufficio di trasformazione o un Cloud Center of Excellence (CCoE). A CCo E sviluppa e promuove un approccio per l'implementazione della tecnologia cloud su larga scala all'interno di un'organizzazione. Per un'adozione efficace del cloud, progetta la tua CCo E in modo da includere rappresentanti in grado di parlare a nome dei team e dei dipartimenti coinvolti. Inizia in piccolo e fai evolvere in modo incrementale l' CCoE per soddisfare le tue esigenze man mano che avanzi nel percorso di trasformazione. I rappresentanti principali del tuo provider di servizi cloud, come il tuo AWS account manager e l'architetto delle soluzioni, possono fornirti risorse per guidarti nella creazione del tuo E. CCo A CCo E accelera la vostra capacità di acquisire competenze in materia, ottenere il consenso, conquistare la fiducia in tutta l'organizzazione e stabilire linee guida efficaci per soddisfare i requisiti

della vostra missione. Non esiste un'unica struttura organizzativa che funzioni per ogni istituto, ma le seguenti domande vi aiuteranno a progettare la vostra E. CCo

- Chi dovresti includere nella tua CCo E?

  All'inizio, una CCo E poteva includere solo una manciata di early adopter e campioni del cloud. La CCo E potrebbe rimanere piccola, ma dovrebbe evolversi per includere campioni in grado di parlare sia a nome delle funzioni aziendali che delle funzioni tecniche interessate dall'adozione del cloud. Le funzioni aziendali comprendono la gestione delle modifiche, i requisiti degli stakeholder, la governance, la formazione, l'approvvigionamento e le comunicazioni. Queste funzioni sono generalmente rappresentate dai membri dei team amministrativi e didattici dell'istituto. Le funzioni tecniche includono infrastruttura, automazione, strumenti operativi, sicurezza, prestazioni e disponibilità. Queste funzioni sono generalmente rappresentate dai membri dei team IT dell'istituto. La CCo E dovrebbe inoltre cercare di coinvolgere fornitori e partner, se necessario, per fornire competenze in materia. La CCo E è un'organizzazione vivente. La sua composizione, forma e funzione probabilmente cambieranno nel tempo e potrebbe persino sciogliersi a un certo punto delle future maturità.
- In che modo l' CCoUE interagisce con i suoi stakeholder?

  La CCo E è al servizio di altri team e ha il solo scopo di informare e consentire un'adozione efficace del cloud. Cerca di incorporare parti della CCo E in vari dipartimenti, scuole e funzioni. Ciò consente l'accesso a una gamma più ampia di risorse e un feedback interno più rapido. Concentrati sulla creazione precoce di partnership e linee di comunicazione aperte tra le parti interessate per stabilire la fiducia all'interno dell'istituto e abbattere i silos organizzativi. L' CCoE dovrebbe avere meccanismi definiti per comunicare con le parti interessate, raccogliere feedback e formare gli utenti. Le metriche di successo dell' CCoUE dovrebbero riflettere tale collaborazione e comunicazione. Se un team si misura solo sulla tecnologia degli edifici, si svilupperà più tecnologia, ma il suo utilizzo e i suoi risultati passeranno in secondo piano. Le tue metriche dovrebbero invece misurare elementi come il numero di team che diventano autosufficienti grazie al lavoro della CCo E, il numero di volte in cui l' CCoE intraprende il percorso decisivo per le iniziative, il numero di eventi di formazione organizzati o il grado di adozione dei risultati della E. CCo Una E ben costruita CCo e affidabile può essere un trampolino di lancio verso una più ampia trasformazione organizzativa basata sulla fiducia.
- Come dovresti stabilire una CCo E?

La maggior parte delle organizzazioni inizia l'adozione del cloud con progetti pilota specifici e mirati. Stabilisci una CCo E come parte di questi progetti. Un buon inizio è fondamentale per definire il successo dell'intero percorso.

- Inizia con un problema aziendale. La tecnologia fine a se stessa è una cattiva strategia. Se stai sperimentando tecnologie cloud, identifica un caso d'uso aziendale convincente, indipendentemente da quanto piccolo possa sembrare. Quindi, riprendi da quel caso d'uso per fissare obiettivi chiari su come la tecnologia può aiutarti. Non implementate la soluzione in un silo. Ricevete input costanti dagli stakeholder aziendali prima e durante l'implementazione del progetto. Tutti i progetti cloud di successo si basano su una stretta collaborazione con le unità istituzionali che utilizzeranno la tecnologia.
- Inizia in piccolo. Scegli un progetto a basso rischio che offra una porta bidirezionale. Ciò significa che il progetto è reversibile e gli eventuali errori possono essere corretti rapidamente. I progetti pilota sono tutti incentrati sulla sperimentazione. Evitare progetti su larga scala e ad alto rischio consente di controllare meglio l'implementazione e i risultati. Aiuta a indirizzare problemi specifici e definibili anziché obiettivi di ampia portata. Ad esempio, se l'automazione è l'obiettivo finale, cerca di automatizzare attività specifiche anziché interi lavori.
- Definisci e misura il risultato. Stabilisci metriche chiare per valutare i progressi e le prestazioni di ogni progetto. Definisci lo stato finale desiderato con largo anticipo per evitare aspettative non corrispondenti tra le parti interessate. Collaborate a stretto contatto con gli stakeholder aziendali e gli altri leader all'interno dell'organizzazione per definire aspettative e guadagni misurabili. È anche importante tradurre i risultati in un linguaggio non tecnico. Parla in termini di obiettivi istituzionali, ad esempio in che modo il progetto ha migliorato la fidelizzazione e ridotto il tasso di abbandono, come ha ridotto i costi e aumentato la velocità di consegna, e così via.
- Inizia dalla zona di comfort. Scegli un progetto all'interno di un dominio che il tuo istituto conosce. In questo modo puoi assicurarti che il progetto abbia obiettivi significativi e comprensibili con un impatto reale. Un progetto di questo tipo rafforzerà la fiducia e produrrà maggiori risultati a lungo termine per l'organizzazione. Ad esempio, se hai già esperienza nell'analisi dei dati, puoi iniziare il tuo percorso verso il cloud sfruttando le tue competenze esistenti iniziando con un progetto di analisi. Ogni istituto ha competenze diverse e deve trovare i suoi componenti unici per elaborare una strategia di trasformazione digitale di successo.

Distinguere tra applicazioni SaaS e servizi cloud di base

La maggior parte degli istituti di istruzione ha già adottato applicazioni SaaS (Software as a Service). Il SaaS fornisce al tuo istituto una soluzione completa gestita e gestita dal fornitore di servizi. Le applicazioni SaaS più comuni includono applicazioni di produttività come l'elaborazione di testi e la posta elettronica, ma esistono anche opzioni SaaS per molti carichi di lavoro cruciali come la pianificazione delle risorse aziendali (ERP), i sistemi informativi per studenti (SIS) e i sistemi di gestione dell'apprendimento (LMS). Quando il tuo istituto adotta un'offerta SaaS, il tuo team IT non deve pensare a come viene mantenuto il servizio o a come viene gestita l'infrastruttura: i tuoi utenti si limitano a fruire del servizio. Questo modello di erogazione riduce l'onere di gestione per il personale IT. Molte istituzioni scelgono di adottare un approccio «SaaS first» nella loro strategia IT, soprattutto se i loro team IT non hanno il tempo, le risorse o le competenze per ospitare in modo sufficientemente autonomo la stessa applicazione. Anche se disponi delle risorse per l'hosting autonomo, potrebbe essere comunque più conveniente adottare una soluzione SaaS e investire invece in altri progetti.

Quando utilizzi applicazioni SaaS, il tuo team IT non deve gestire l'infrastruttura sottostante, quindi il luogo in cui il fornitore ospita l'applicazione (data center locale, provider cloud principale o un provider cloud alternativo) diventa meno importante. Dopo aver scelto un provider cloud primario e strategico, puoi scegliere di utilizzare un'offerta SaaS ospitata in un altro provider di cloud o on-premise, nel data center del fornitore. Al contrario, anche se le tue applicazioni SaaS sono ospitate in un provider cloud, potresti scegliere un provider cloud primario e strategico diverso in base alla forza di quel provider per i tuoi carichi di lavoro non SaaS. La distinzione tra ambienti di hosting è meno importante per SaaS che per le applicazioni self-hosted. Tuttavia, dovresti comunque considerare le seguenti domande chiave quando valuti in che modo il SaaS si adatta al cloud come parte della tua strategia IT.

- L'applicazione SaaS è altamente disponibile e scalabile?

  Molti fornitori hanno già deciso di adottare il cloud per le loro offerte SaaS. In tal modo, il fornitore è in grado di ottenere i vantaggi del cloud derivanti da una maggiore disponibilità e scalabilità. Inoltre, poiché il fornitore può adottare il modello di responsabilità condivisa del cloud anziché gestire e mantenere l'infrastruttura fisica, può investire più tempo e risorse nella fornitura di nuove funzionalità. Grazie a questi vantaggi, dovresti preferire provider che si concentrano sul cloud e che offrono soluzioni ospitate nel cloud.
- L'applicazione SaaS può soddisfare i tuoi requisiti di sicurezza?

Quando si valuta una soluzione SaaS, è importante sapere quali dati vengono archiviati dall'applicazione, come vengono utilizzati e quali controlli di sicurezza sono in atto per proteggere tali dati. Anche se potresti non avere il controllo diretto sull'archiviazione dei dati come avresti nel tuo ambiente ospitato autonomamente, dovresti assicurarti che il fornitore disponga di meccanismi e controlli per gestire i tuoi dati in modo appropriato. Tieni presente quali funzionalità di sicurezza sono integrate nella soluzione SaaS e quali funzionalità richiedono una configurazione aggiuntiva. Il cloud consente ai provider SaaS di creare soluzioni più disponibili e scalabili e possono anche creare soluzioni più sicure grazie al modello di responsabilità condivisa. Dovresti preferire fornitori che sfruttano gli strumenti e i servizi di sicurezza del cloud come parte delle loro soluzioni.

- Chi possiede i dati delle applicazioni SaaS e come è possibile accedervi?

  Quando utilizzi SaaS, ti fidi che il provider gestisca correttamente i dati del tuo istituto. Assicurati di leggere i termini di servizio e gli accordi sui livelli di servizio per le applicazioni SaaS per comprendere i fattori che contribuiscono come la proprietà, la disponibilità e la durabilità dei dati. Valuta i meccanismi per il backup o l'esportazione dei dati; questi sono particolarmente importanti nel caso in cui decidessi di cambiare fornitore o il provider interrompa il servizio.

- Gli altri servizi e le applicazioni self-hosted possono integrarsi con l'applicazione SaaS, indipendentemente dall'ambiente?

  Quando si adotta una soluzione SaaS, è facile presumere che i servizi e le applicazioni che condividono lo stesso ambiente di hosting (ovvero applicazioni che utilizzano lo stesso provider di cloud o il data center dello stesso fornitore) avranno un'integrazione più semplice. Tuttavia, la maggior parte delle soluzioni SaaS oggi offre un ampio supporto per API e integrazioni di terze parti, quindi non limitarti a soluzioni ospitate nello stesso ambiente. Se esistono le integrazioni necessarie, le soluzioni non devono necessariamente condividere lo stesso ambiente sottostante. Ad esempio, supponiamo che tu stia utilizzando una soluzione SaaS come Google Drive o Microsoft OneDrive per l'archiviazione dei file degli studenti basata sul cloud. Per fornire desktop virtuali e streaming di applicazioni ai tuoi studenti, potresti decidere che Amazon WorkSpaces Applications sia la soluzione migliore per le tue esigenze. Sebbene questi servizi vengano eseguiti in ambienti diversi, WorkSpaces Applications offre integrazioni native con Google Drive e Microsoft OneDrive, in modo che gli studenti possano continuare a utilizzare lo spazio di archiviazione esistente.

- L'applicazione SaaS supporta la gestione centralizzata delle identità?

  Per evitare che il tuo team IT debba gestire diversi archivi di identità e che gli utenti debbano ricordare più set di credenziali, assicurati che le tue soluzioni SaaS supportino l'integrazione con

le soluzioni esistenti di gestione delle identità o Single Sign-On. La gestione frammentata delle identità riduce la produttività e può portare a pratiche di sicurezza scorrette, come privilegi creep e password deboli. Se la soluzione SaaS desiderata non supporta il Single Sign-On o l'archivio di identità esistente, valuta se il valore aziendale dell'adozione della soluzione supera il maggiore onere per utenti e personale.

- Come è possibile proteggere la comunicazione di rete con l'applicazione SaaS?

  In alcuni casi, potrebbe essere necessaria un'applicazione self-hosted per comunicare con un'applicazione SaaS. In genere, questa comunicazione avverrà tramite APIs e sarà protetta con meccanismi di autenticazione e autorizzazione appropriati. Tuttavia, a seconda degli ambienti di hosting delle due applicazioni, potrebbero essere necessari meccanismi alternativi o aggiuntivi per semplificare o proteggere tale comunicazione. Ad esempio, se offri l'hosting autonomo di un'applicazione presso un provider di servizi cloud e devi integrarla con un'applicazione SaaS ospitata sullo stesso provider di servizi cloud, il fornitore potrebbe fornire diverse opzioni di connessione. Potresti essere in grado di utilizzare connessioni peering specifiche per il cloud, interfacce private o private APIs, AWS PrivateLinkper impedire che tali comunicazioni attraversino la rete Internet pubblica. Allo stesso modo, se l'applicazione locale dispone di una connessione di rete dedicata a un provider di servizi cloud tramite un servizio come AWS Direct Connect, è possibile utilizzare la stessa connessione per comunicare con le applicazioni SaaS ospitate sullo stesso provider cloud.

Stabilisci i requisiti di sicurezza e governance per ogni provider di servizi cloud

Gli istituti di istruzione hanno una serie di obiettivi di conformità, governance e sicurezza informatica che devono raggiungere. I rischi del mancato raggiungimento di questi obiettivi possono includere la perdita della reputazione istituzionale, multe pecuniarie, riscatti, violazioni di dati sensibili, furto di proprietà intellettuale e perdita degradata o totale di funzioni cruciali. Grazie al modello di responsabilità condivisa, gli istituti che adottano i servizi cloud possono ridurre gli oneri amministrativi scaricando parte della responsabilità della sicurezza dell'infrastruttura sul fornitore di servizi cloud. Inoltre, puoi beneficiare di servizi di sicurezza specifici e nativi del cloud che offrono funzionalità spesso non disponibili, difficili da gestire o proibitive in termini di costi in un'implementazione locale. Alcuni esempi includono servizi come AWS WAFla protezione delle applicazioni Web, AWS Shieldla protezione Distributed Denial of Service (DDoS) e Amazon GuardDuty per il rilevamento delle minacce. Una strategia di sicurezza e governance del cloud efficace consente ai team IT e

di sicurezza di concentrarsi sulla creazione di sistemi sicuri fin dalla progettazione, aiuta l'istituto ad adattarsi rapidamente ai requisiti di missione in evoluzione e fornisce a docenti e ricercatori ambienti sicuri per l'apprendimento e l'innovazione rivoluzionari. Per valutare i requisiti di sicurezza e governance, considera le seguenti domande chiave.

- A quali framework di conformità devono allinearsi i carichi di lavoro?

  Gli istituti di istruzione devono aderire a molti quadri di conformità a causa della moltitudine di parti interessate e dei carichi di lavoro che supportano. Questi quadri di conformità includono il Family Educational Rights and Privacy Act (FERPA), l'Health Insurance Portability and Accountability Act (HIPAA), il Federal Risk and Authorization Management Program (FedRAMP), la Cybersecurity Maturity Model Certification (CMMC), l'International Traffic in Arms Regulations (ITAR), il Criminal Justice Information Services (CJIS) e il Payment Card Industry Data Security Standard (PCI). DSS). In alcuni casi, ad esempio con CMMC, i finanziamenti per le sovvenzioni per la ricerca non vengono erogati fino a quando i carichi di lavoro pertinenti non vengono certificati come conformi. Ogni framework è unico e può essere applicato solo a un sottoinsieme di carichi di lavoro. Assicurati di sapere quali carichi di lavoro devono rispettare quali requisiti e di essere in grado di soddisfare tali requisiti nell'ambiente di ciascun carico di lavoro. Negli ambienti cloud, assicurati di comprendere le tue responsabilità rispetto a quelle del provider di servizi cloud. È necessario disporre delle conoscenze, delle risorse e delle competenze necessarie per raggiungere e mantenere la conformità.
- Quali meccanismi disponi per far rispettare la conformità tra più provider di cloud senza inibire l'innovazione?

  Se il tuo istituto accademico è alle prime armi con il cloud, ti consigliamo di scegliere un fornitore di servizi cloud strategico primario e di concentrarti sulla comprensione di come progettare, progettare e gestire ambienti cloud che siano sicuri fin dalla progettazione. Idealmente, i controlli di sicurezza che vengono incorporati automaticamente nei sistemi self-service consentono agli utenti di implementare rapidamente ambienti cloud sicuri con un intervento minimo da parte dei team IT. Concentrarsi su un unico provider limita la quantità di risorse e tempo da investire per garantire sicurezza e conformità. Gli istituti di maggior successo scelgono un provider di servizi cloud in grado di supportare la maggior parte dei requisiti di conformità, dispone di una solida rete di partner, offre soluzioni di conformità predefinite e rende disponibile l'automazione self-service sicura. Se è necessario garantire la sicurezza e la conformità tra più provider di cloud, saranno necessari investimenti aggiuntivi per sviluppare le competenze e le risorse necessarie per gestire la conformità per ogni ambiente. Se ogni provider di cloud utilizza un ambiente di base, o landing zone, diverso, devi capire quali standard e requisiti di conformità può supportare

ciascuna landing zone e ciò potrebbe determinare se determinati carichi di lavoro possono essere ospitati su quel provider. È possibile gestire la conformità per ciascun provider separatamente o utilizzare soluzioni personalizzate o realizzate da partner in grado di centralizzare la gestione tra i provider. Marketplace AWSfornisce soluzioni chiavi in mano in grado di soddisfare anche i requisiti di conformità.

- Come è possibile valutare e controllare i costi e l'utilizzo tra più provider di cloud?

  Se il tuo istituto accademico è alle prime armi con il cloud, ti consigliamo di stabilire meccanismi di visibilità e controllo dei costi per ottenere informazioni dettagliate su quali servizi cloud vengono utilizzati, a chi appartengono le risorse cloud, qual è lo scopo di tali risorse cloud e quali potenziali risparmi sui costi si possono ottenere ottimizzando i consumi. Gli istituti possono ottenere un significativo ritorno sull'investimento collaborando con il proprio provider di servizi cloud per migrare e modernizzare i sistemi mission-critical, poiché possono negoziare accordi a livello aziendale, beneficiare dei prezzi basati sui volumi e sfruttare l'esperienza del fornitore di servizi cloud. Se devi controllare i costi e l'utilizzo tra più provider, considera come aggregare e analizzare i costi e l'utilizzo di ciascun provider, utilizzando processi e strumenti interni o utilizzando soluzioni partner. Molte organizzazioni stanno iniziando a identificare le operazioni finanziarie nel cloud (FinOps) come una funzione chiave e stanno dedicando risorse alla diffusione e all'implementazione di funzionalità per la gestione e l'ottimizzazione dei costi del cloud.
- Disponete di meccanismi per gestire facilmente le autorizzazioni degli utenti nel tempo?

  Consigliamo agli istituti accademici di comprendere le esigenze principali delle parti interessate quando si avvicinano per la prima volta al cloud. Gli utenti dei sistemi istituzionali includono studenti, docenti, ricercatori, personale IT, amministrazione, sicurezza, pubblico in generale e collaboratori di terze parti. È necessario identificare le esigenze principali di questi utenti e assicurarsi di disporre di meccanismi appropriati per concedere loro l'accesso ai servizi cloud. Tipi diversi di utenti richiedono tipi diversi di accesso ai servizi cloud. Ad esempio, gli studenti, i docenti e il pubblico in generale devono accedere alle applicazioni; il personale IT, gli amministratori e gli addetti alla sicurezza devono accedere all'infrastruttura cloud; i ricercatori e i loro collaboratori terzi devono accedere ad ambienti di ricerca sicuri; i docenti devono accedere ad ambienti di insegnamento sicuri e potrebbero persino voler fornire agli studenti un accesso pratico alle tecnologie cloud. È necessario disporre di strumenti per gestire centralmente queste identità in modo automatizzato e utilizzare processi consolidati per identificare, concedere e revocare le autorizzazioni man mano che ruoli e responsabilità cambiano nel tempo.
- Disponete di meccanismi per integrare in modo appropriato i nuovi sistemi con la vostra soluzione di gestione delle identità?

Consigliamo agli istituti accademici di semplificare l'integrazione di nuovi sistemi con i propri sistemi di gestione delle identità. Ciò offre all'istituto la flessibilità necessaria per supportare una serie di funzioni cruciali, consentendo alle parti interessate di procurarsi e creare sistemi che possono essere facilmente integrati nel sistema di gestione delle identità. Semplificando il processo di integrazione, le parti interessate saranno meno propense a utilizzare le proprie misure di controllo degli accessi, che potrebbero non applicare le migliori pratiche di sicurezza come single sign-on, passkey e autenticazione a più fattori (MFA). Assicurati che il tuo sistema di gestione delle identità possa interagire con i sistemi necessari tramite integrazioni native o protocolli standard del settore.

- Disponete di meccanismi per consentire un rilevamento e una risposta efficaci agli incidenti?

  Gli istituti scolastici sono spesso bersaglio di attacchi informatici e ransomware. Per aiutare a rilevare e rispondere efficacemente a tali incidenti, consigliamo un approccio biforcato:

  - Concentra i tuoi sforzi sulle misure preventive sotto forma di controlli di sicurezza che vengono automaticamente incorporati negli ambienti cloud.
  - Implementa funzionalità di rilevamento che aiutino i soccorritori agli incidenti informatici a rilevare, contenere e mitigare tempestivamente le violazioni della sicurezza.

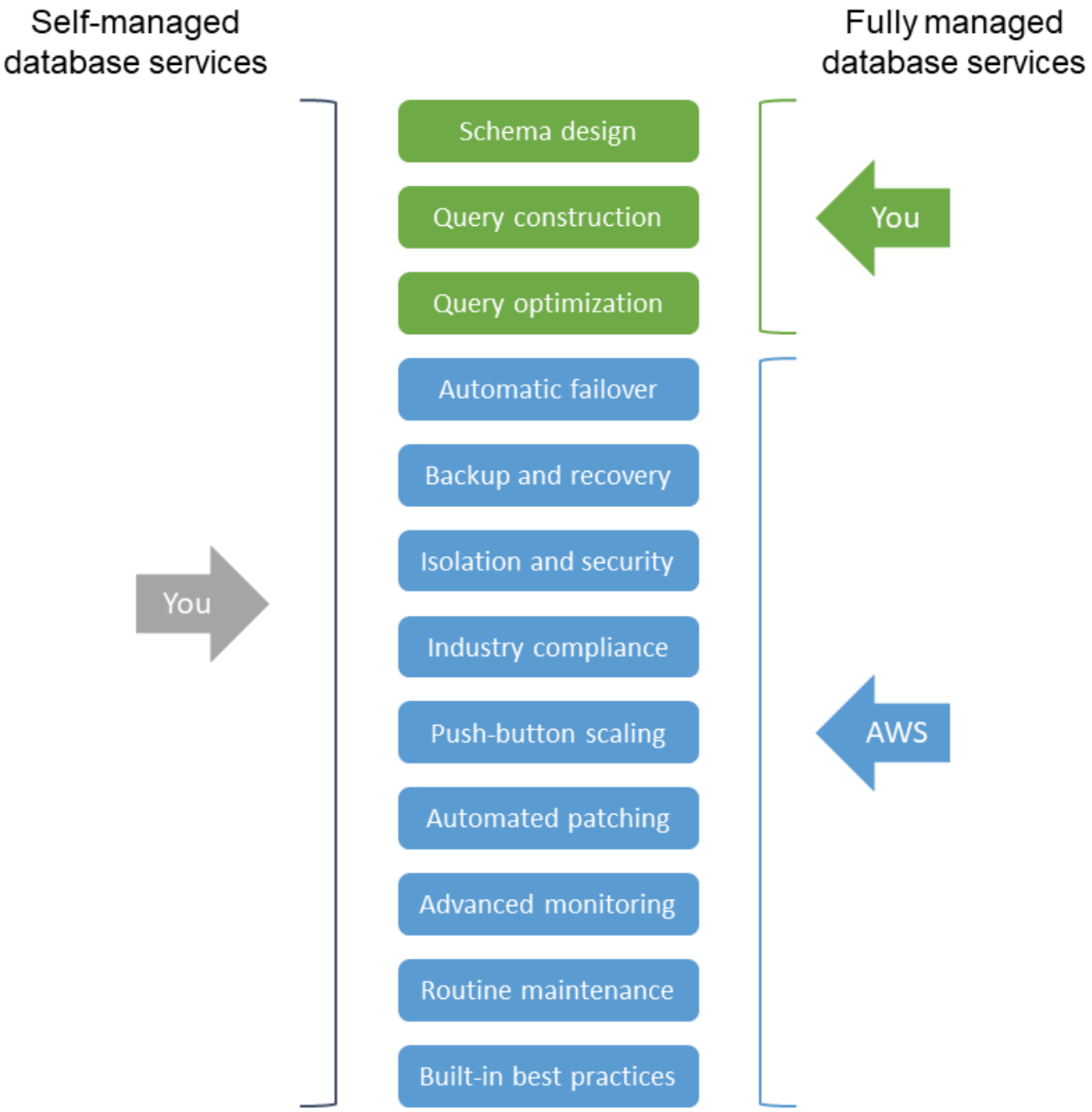
Per quanto riguarda la conformità, è necessario assicurarsi di disporre delle risorse, delle competenze e degli strumenti per rilevare, prevenire e rispondere agli eventi in ogni ambiente. Concentrandoti su un unico provider di cloud primario, puoi limitare le risorse necessarie. Le istituzioni accademiche che non dispongono di un team addetto alle operazioni di sicurezza dovrebbero rivolgersi a fornitori di software indipendenti, fornitori di servizi gestiti di rilevamento e risposta e consulenti in materia di sicurezza informatica per ricevere assistenza in queste aree.

Adotta servizi gestiti nativi per il cloud laddove possibile e pratico

Se inizialmente consideri come sfruttare i servizi cloud, utilizzare i servizi di infrastruttura e gli strumenti di sviluppo che i tuoi team conoscono potrebbe sembrare la strada migliore da seguire. Tuttavia, la selezione di servizi gestiti nativi del cloud, in particolare le opzioni serverless, può ridurre notevolmente costi, impegno e complessità.

I servizi gestiti nativi per il cloud eliminano molte delle attività IT indifferenziate che richiedono tempo e impegno da parte del personale e che potrebbero essere impiegate meglio in attività incentrate sulla missione. Inoltre, man mano che i provider migliorano le funzionalità dei propri servizi, le vostre soluzioni ereditano naturalmente miglioramenti incrementali in termini di efficienza, sicurezza,

resilienza, prestazioni e altre caratteristiche. Ad esempio, un servizio di database completamente gestito è un sistema di gestione di database relazionali ricco di funzionalità, ma non è necessario fornire e gestire il server e il sistema operativo sottostanti su cui viene eseguito il database. Ciò elimina le attività amministrative che in genere sono necessarie quando si mantiene un database relazionale nel proprio data center o su un server virtuale autogestito fornito nel cloud. Il diagramma seguente illustra questa differenza.



I vantaggi dell'eliminazione della gestione dell'infrastruttura sono evidenti se si confronta qualsiasi servizio gestito nativo del cloud con un approccio autogestito analogo. Di conseguenza, ogni volta che è necessario implementare componenti su cui eseguire le applicazioni acquistate o sviluppate su misura, è necessario utilizzare servizi gestiti nativi del cloud per ridurre tempi e sforzi.

Se il tuo team è responsabile della creazione, dell'implementazione o della gestione di soluzioni nel cloud, utilizza i servizi gestiti nativi del cloud per sfruttare appieno le funzionalità e le innovazioni differenziate del tuo provider di servizi cloud. Questa strategia consente di selezionare, integrare e implementare i servizi cloud in modo da ridurre il tempo e l'impegno richiesti da questi progetti, aumentandone al contempo la resilienza e la sicurezza. Per una strategia cloud di successo, prendi in considerazione l'adozione di questi elementi costitutivi nativi del cloud quando migri soluzioni personalizzate sul cloud, sviluppi nuove soluzioni nel cloud o distribuisci software con licenza sul cloud. Quando valuti le opzioni per i servizi gestiti nativi del cloud, considera le seguenti domande chiave.

- Avete bisogno di concentrare maggiormente il tempo e gli sforzi del vostro personale sulle funzionalità che sono fondamentali per la vostra missione educativa?

  La gestione dei server, anche quelli virtuali, richiede tempo e attenzione per garantire che rimangano aggiornati con gli aggiornamenti e le patch del software di sistema. L'utilizzo di servizi gestiti che gestiscono queste attività al posto vostro consente di indirizzare il tempo del personale IT verso attività che si allineano più direttamente alla missione del vostro istituto. Ad esempio, se devi implementare container, prendi in considerazione un servizio gestito senza server, AWS Fargatein modo da non dover configurare e gestire i server. Eliminando la necessità di acquistare, fornire e gestire l'infrastruttura sottostante, puoi concentrarti invece sulla fornitura di nuove funzionalità, sull'ottimizzazione delle prestazioni e sul miglioramento dell'esperienza utente. Considerate questo vantaggio quando valutate i servizi gestiti rispetto alle opzioni autogestite.
- Che impegno occorrerà al tuo team per adottare servizi gestiti nativi del cloud?

  La progettazione e l'implementazione di soluzioni con servizi gestiti nativi per il cloud possono richiedere una curva di apprendimento, ma questi sforzi saranno ripagati con riduzioni di costi, tempi e complessità nel corso del ciclo di vita di una soluzione. Grazie alla pay-as-you-go natura on-demand del cloud computing, i servizi nativi del cloud consentono di iterare e sperimentare rapidamente in modo più agile evitando investimenti iniziali. Ciò porta a una maggiore innovazione e a tempi di progetto più brevi. Tuttavia, per ottenere questi vantaggi in modo efficace, prendete in considerazione le possibilità di adottare e utilizzare il servizio, ad esempio la formazione del personale sui modelli di utilizzo ottimali e il refactoring del codice per adattarlo a esigenze specifiche del servizio. APIs Anche se il servizio utilizza standard di settore o open source APIs, potrebbe essere necessario rifattorizzare o configurare l'applicazione per gestire le disparità di funzionalità o le mancate corrispondenze tra le versioni.
- Come si implementa e gestisce attualmente l'infrastruttura? È necessario mantenere quel livello di controllo?

Esistono diversi modi per ospitare e gestire l'infrastruttura nel cloud, incluso l'utilizzo di host bare-metal, macchine virtuali, servizi di container gestiti e offerte serverless. Anche se attualmente utilizzi un'infrastruttura simile, come macchine virtuali o contenitori, nel tuo ambiente locale, valuta se un approccio alternativo sarebbe adatto per determinati carichi di lavoro. Ad esempio, invece di eseguire tutte le applicazioni su macchine virtuali, prendi in considerazione la containerizzazione delle applicazioni e sfrutta i servizi di container gestiti come Amazon Elastic Container Service (Amazon ECS). Ciò potrebbe richiedere il refactoring, ma puoi utilizzare uno strumento come quello AWS App2Containerper semplificare e agevolare la containerizzazione. Facendo un ulteriore passo avanti, invece di implementare server o contenitori per tutti i componenti, prendi in considerazione opzioni completamente serverless. Le tecnologie serverless offrono scalabilità automatica, alta disponibilità integrata e un modello di pay-for-use fatturazione per aumentare l'agilità e ottimizzare i costi. Allo stesso tempo, eliminano la necessità di gestire i server e pianificare la capacità. Servizi di elaborazione serverless, ad esempio quelli fondamentali per AWS Lambdale architetture serverless. Lambda supporta linguaggi di programmazione comuni e consente agli sviluppatori di concentrarsi sul codice dell'applicazione anziché sulla gestione dell'infrastruttura. Esplora queste opzioni per ogni carico di lavoro e considera fattori come la curva di apprendimento, il sovraccarico di gestione, i costi e le licenze.

- Devi implementare e gestire l'infrastruttura per qualsiasi software concesso in licenza?

  Quando distribuisci e gestisci software concesso in licenza da fornitori di software indipendenti (ISVs), potrebbe sembrare logico imitare la distribuzione locale con un'infrastruttura cloud. Ad esempio, potresti prendere in considerazione la possibilità di sostituire le macchine virtuali locali con macchine virtuali ospitate nel cloud. Sebbene si tratti di un'opzione valida, valuta se puoi sostituire qualsiasi componente dell'architettura con servizi gestiti nativi del cloud. Ad esempio, potresti essere in grado di sostituire un server di database autogestito con un servizio di database completamente gestito che riduca gli oneri amministrativi utilizzando lo stesso motore di database. Molti utilizzano ISVs già architetture cloud che sfruttano i servizi gestiti e potrebbero persino offrire modelli predefiniti per semplificare l'implementazione. Ove possibile, dovresti preferire ISVs che offrano indicazioni e supporto prescrittivi per le implementazioni cloud. Prima di distribuire il software con licenza sul cloud, assicurati di consultare il tuo ISV per capire in che modo le licenze dell'ambiente cloud potrebbero differire dalle licenze locali.
- Temi che l'utilizzo di un servizio gestito possa comportare il vincolo del fornitore?

  Molti servizi gestiti nativi del cloud sono progettati per supportare standard di settore comuni e. APIs Ad esempio, i servizi di analisi come AWS GlueAmazon EMR si basano su framework di elaborazione e archiviazione standard del settore come Apache Spark e Apache Parquet. AWS

Lambdasupporta nativamente codice Java, Go, Microsoft PowerShell, Node.js, C#, Python e Ruby. Amazon Relational Database Service (Amazon RDS) supporta più versioni di motori di database comuni, tra cui SQL Server, Oracle, PostgreSQL e MySQL. Quando i servizi dispongono di soluzioni proprietarie APIs, native o partner, potrebbero essere disponibili soluzioni con cui interagire utilizzando protocolli comuni indipendenti dal cloud. APIs Ad esempio, Amazon Simple Storage Service (Amazon S3) dispone di un'API specifica del servizio per l'integrazione diretta, ma puoi anche interagire con essa utilizzando protocolli di storage standard come Network File System (NFS), Server Message Block (SMB) e Internet Small Computer Systems Interface (iSCSI) quando si utilizza. Gateway di archiviazione AWS Dovresti comunque concentrarti sulla scelta del servizio gestito nativo del cloud che meglio soddisfa le tue esigenze riducendo al contempo il sovraccarico operativo, ma potresti preferire servizi che utilizzano o rendono disponibili standard e protocolli di settore comuni.

Implementa architetture ibride laddove esistenti, gli investimenti locali incentivano l'uso continuato

La maggior parte degli istituti di istruzione ha investito in data center locali di varia scala per ospitare applicazioni aziendali, soluzioni di archiviazione dati, ambienti di elaborazione per utenti finali (EUC) e risorse informatiche condivise. Tutte le risorse di questi data center sono soggette a diversi cicli di aggiornamento, in cui è necessario considerare la crescita futura e fornire una capacità sufficiente per soddisfare i picchi di scala, che potrebbero essere necessari solo poche volte all'anno. Di conseguenza, le risorse spesso rimangono inattive fino al ciclo di aggiornamento successivo. La pianificazione, la definizione del budget, l'approvvigionamento e l'installazione di nuovo hardware possono richiedere settimane, se non mesi o più. Questo lungo processo soffoca l'innovazione e può ritardare l'apprendimento e la ricerca.

Il cloud computing risolve molte di queste sfide. Il cloud fornisce risorse pay-as-you-go IT su richiesta, in modo da poter abbinare più da vicino la capacità attuale con le richieste effettive senza una pianificazione e un investimento ingenti e iniziali. Tuttavia, se hai già fatto un investimento significativo in hardware e risorse locali, dovresti cercare di utilizzare tali risorse in modo efficiente e aumentarle secondo necessità con la tecnologia cloud in un modello ibrido.

Una strategia di cloud ibrido di successo sfrutta gli investimenti esistenti fornendo al contempo maggiore agilità, scalabilità e affidabilità rispetto a quelle supportate da soli investimenti. Le seguenti considerazioni possono aiutarti a iniziare.

- Quando devi ospitare un nuovo carico di lavoro, pensi innanzitutto al cloud?

  Il modo in cui utilizzi insieme l'infrastruttura cloud pubblica e privata definisce la tua strategia di cloud ibrido. Un approccio incentrato sul cloud non significa che il cloud sia la scelta migliore per tutti i carichi di lavoro. Tuttavia, quando pianifichi nuovi carichi di lavoro, valuta il cloud come prima opzione, in particolare per i carichi di lavoro che richiedono nuove tecnologie o superano la capacità di archiviazione ed elaborazione disponibile in locale. I carichi di lavoro che presentano modelli di utilizzo transitori e incoerenti, richiedono risultati rapidi, sono facilmente trasportabili o richiedono l'hardware più recente sono i candidati ideali per la scalabilità e l'elasticità del cloud. Inoltre, valuta se il carico di lavoro trarrebbe vantaggio da servizi gestiti nativi del cloud che non sono disponibili in sede, anche se disponi di capacità disponibile.
- Conoscete il TCO del vostro ambiente locale e collaborate con il vostro CFO per effettuare nuovi investimenti?

  Ti consigliamo di comprendere il vero costo totale di proprietà (TCO) della manutenzione del tuo data center locale. Esistono molti costi nascosti associati alla proprietà e alla gestione dell'infrastruttura locale, tra cui non solo hardware, software e supporto, ma anche strutture, servizi di pubblica utilità, assicurazioni e orari del personale. Questi costi possono influire negativamente sulla produttività del personale, sulla resilienza operativa e sull'agilità aziendale. Valuta anche le tue attuali strutture di licenza e i relativi periodi di rinnovo e manutenzione. La collaborazione con il vostro Chief Financial Officer (CFO) può aiutarvi a identificare tutti i costi nascosti quando pianificate di effettuare nuovi investimenti. Alcune licenze potrebbero offrire opzioni Bring Your Own License (BYOL) nel cloud oppure potrebbero essere più o meno favorevoli ai servizi cloud. Comprendere il vero TCO della tua infrastruttura attuale ti aiuta a dare priorità all'adozione del cloud per i carichi di lavoro che hanno il maggiore impatto sul TCO totale dell'organizzazione. Il tuo team addetto all' AWS account dispone di strumenti immediatamente disponibili per aiutarti a comprendere meglio il TCO locale.
- Di quale infrastruttura avrai bisogno per supportare le implementazioni ibride?

  Per adottare con successo i modelli ibridi, avrai bisogno di strumenti di base per la rete, la sicurezza e l'infrastruttura. Assicurati di poter mantenere una connettività di rete adeguata con il tuo provider di servizi cloud. Ciò potrebbe avvenire attraverso una combinazione di connettività Internet esistente, reti private virtuali (VPNs), connessioni dedicate come Direct Connect fornitori di connettività di terze parti o Internet2 e reti regionali di ricerca e istruzione. Assicurati di disporre di una gestione unificata delle identità e degli accessi negli ambienti locali e cloud. Stabilisci strumenti e processi per applicare barriere coerenti in materia di sicurezza, costi e utilizzo.

- Il personale IT è pronto a gestire implementazioni ibride?

  I servizi cloud possono richiedere competenze specifiche che il tuo team potrebbe non avere. Per limitare la formazione e l'abilitazione necessarie per migliorare le competenze del personale IT per un'efficace adozione del cloud, valuta se il provider di servizi cloud offre servizi che riutilizzano e si basano sulle competenze esistenti in locale e nel cloud. Ad esempio, se usi e conosci Kubernetes, potresti prendere in considerazione l'utilizzo di Amazon Elastic Kubernetes Service (Amazon EKS) o Amazon EKS Anywhere. Se usi e conosci bene NetApp, potresti prendere in considerazione l'idea di utilizzare Amazon FSx for NetApp ONTAP. Allo stesso modo, valuta anche se le soluzioni partner esistenti che utilizzi dispongono di integrazioni o supporto nativi per ambienti cloud.

- Puoi trasferire lo storage a lungo termine o l'elaborazione a basso utilizzo dall'ambiente on-premise al cloud?

  L'archiviazione nel cloud offre diverse opzioni convenienti per l'archiviazione dei dati a lungo termine. Ad esempio, Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) offre diversi livelli di storage ottimizzati per diversi casi d'uso. Se il tuo istituto è tenuto a conservare determinati dati per un lungo periodo di tempo, prendi in considerazione soluzioni di conservazione a freddo come Amazon Glacier. Lo scaricamento di questi dati nel cloud storage può liberare prezioso spazio di archiviazione locale ad alte prestazioni. Servizi come Gateway di archiviazione AWSsemplificano l'accesso delle applicazioni locali ai livelli di archiviazione cloud tramite protocolli standard come SMB, NFS e iSCSI. Analogamente, prendi in considerazione la possibilità di scaricare le attività di elaborazione che hanno un utilizzo poco frequente o scarso. Se disponi di server locali dedicati a tali attività, puoi invece utilizzare servizi di cloud computing scalabili, in cui le risorse vengono fornite su richiesta e paghi solo per ciò che usi. Queste opzioni di archiviazione a basso costo e a lungo termine e di elaborazione a basso utilizzo rendono il cloud ideale anche per il backup e il disaster recovery. Puoi utilizzare lo storage e l'elaborazione sicuri, durevoli e scalabili nel cloud per proteggere i tuoi dati e ripristinarli rapidamente in caso di emergenza senza dover mantenere personalmente l'infrastruttura di archiviazione ed elaborazione necessaria.

- Disponi di capacità locale sufficiente per sperimentare e innovare?

  La mancanza di elasticità e agilità negli ambienti locali a dimensione fissa può limitare i servizi e la tecnologia disponibili per gli utenti. Se hai cicli di aggiornamento rigorosi, per l'implementazione dei nuovi carichi di lavoro potrebbe essere necessario attendere il ciclo successivo. Questo modello operativo può limitare la sperimentazione e rallentare l'innovazione. Quando hai un carico di lavoro nuovo o nuovo che deve essere testato, prendi in considerazione l'utilizzo di servizi cloud scalabili ed elastici. È possibile effettuare il provisioning e il deprovisioning delle risorse cloud su richiesta

e si paga solo per ciò che si utilizza, in modo da sperimentare e fallire rapidamente riducendo al minimo i rischi organizzativi.

- Hai requisiti di conformità o prestazioni unici che ti obbligano a conservare i dati on-premise?

  I carichi di lavoro con requisiti rigorosi di residenza o latenza dei dati potrebbero richiedere la conservazione dei dati in locale o il più vicino possibile agli utenti. In questi casi d'uso, puoi dare priorità all'uso delle risorse locali esistenti. Tuttavia, valuta se il tuo provider di servizi cloud offre servizi o meccanismi perimetrali per utilizzare la tecnologia basata sul cloud in locale. I servizi edge offrono l'elaborazione, l'analisi e l'archiviazione dei dati più vicini ai tuoi endpoint e ti consentono di implementare strumenti al di fuori dei data center standard dei provider di cloud. Ad esempio, AWS offre servizi come AWSAWS WavelengthLocal Zones e la distribuzione di applicazioni in luoghi specifici più vicini agli utenti finali. Puoi anche portare servizi e funzionalità cloud nel tuo data center esistente con servizi come AWS OutpostsAmazon ECS Anywhere e Amazon EKS Anywhere. Gateway di archiviazione AWS

Riserva il multicloud solo ai carichi di lavoro che non sono in grado di soddisfare i requisiti tecnici o aziendali tramite un unico provider di servizi cloud

Il multicloud si riferisce all'uso di servizi cloud di più (due o più) provider di servizi cloud. Avere una strategia multicloud può offrire alcuni vantaggi, come la possibilità di sbloccare le funzionalità differenziate di più provider di cloud o la capacità di soddisfare requisiti di sovranità dei dati che un singolo provider di cloud potrebbe non essere in grado di soddisfare. Tuttavia, per ogni provider che utilizzi, assicurati di disporre delle persone, delle competenze, della formazione e dei set di strumenti adeguati per utilizzare quel provider in modo efficace. Inoltre, se desideri utilizzare una strategia multicloud per un carico di lavoro specifico, avrai bisogno di risorse aggiuntive per integrare e interoperare i servizi necessari di ciascun provider di cloud. Ti consigliamo di prendere in considerazione il multicloud solo quando i vantaggi superano l'aumento dell'investimento. Per determinare se scegliere una strategia multicloud, considera le seguenti domande chiave.

- Disponi delle risorse e delle competenze per navigare tra i servizi offerti da diversi provider di cloud?

  Quando più provider di servizi cloud offrono diversi prodotti e servizi, il personale ha bisogno di competenze essenziali per sfruttare le funzionalità di ciascun provider. L'utilizzo dei soli servizi di un provider di servizi cloud può richiedere il miglioramento delle competenze e la formazione del

personale, a seconda dei servizi e delle funzionalità utilizzati. Se stai considerando una strategia multicloud, valuta le tue risorse esistenti per determinare di quali competenze aggiuntive avresti bisogno per utilizzare in modo efficace i servizi di più provider di cloud. Potrebbe essere necessario aumentare il personale o investire tempo e denaro aggiuntivi nell'aggiornamento delle competenze e nella formazione oltre a quanto sarebbe richiesto per un singolo provider di cloud. Se disponi già di singoli team o utenti che utilizzano diversi provider di cloud, valuta i vantaggi organizzativi derivanti dal consolidamento su un unico provider di cloud primario. case-by-case

- Quale sovraccarico aggiuntivo introdurrebbe una particolare architettura multicloud?

  Un fattore comune per il multicloud è il desiderio di utilizzare uno specifico servizio gestito di un provider con funzionalità che possono essere differenziate dai servizi di un altro provider cloud. Ad esempio, potresti voler utilizzare un provider cloud per le tue esigenze di infrastruttura e il servizio gestito di un altro provider per i servizi di dominio e directory. Tuttavia, anche se un unico servizio gestito riduce gli oneri amministrativi e semplifica la gestione di quel componente dell'architettura, potrebbe comportare costi aggiuntivi per altri carichi di lavoro, come il refactoring del codice, le esigenze di connettività privata o il lavoro di integrazione manuale. Identifica subito questo sovraccarico aggiuntivo e assicurati che non compensi o offuschi i vantaggi che il tuo team può trarre dal servizio differenziato.
- Come centralizzerai il monitoraggio e la gestione tra i provider di cloud?

  Quando inizierai a implementare applicazioni e funzionalità utilizzando risorse di diversi provider di servizi cloud, considera come etichettare, monitorare e gestire tali risorse. Ogni provider avrà i propri strumenti, che potresti essere in grado di estendere ad altri ambienti. Ad esempio, puoi utilizzare Amazon per CloudWatch monitorare parametri e log chiave, creare allarmi e visualizzare le tue applicazioni e l'infrastruttura in ambienti singoli, ibridi e multicloud. Puoi anche utilizzarlo AWS Systems Managerper migliorare la visibilità e il controllo delle risorse, diagnosticare e risolvere rapidamente i problemi operativi e automatizzare processi come l'aggiornamento e l'applicazione di patch alle macchine virtuali in tutti gli ambienti. Se hai requisiti che gli strumenti di un provider non sono in grado di supportare, puoi esplorare le soluzioni dei partner, ma queste potrebbero comportare costi o sforzi di integrazione aggiuntivi.
- Come è possibile gestire l'infrastruttura come codice con automazione quando si utilizzano diversi provider di cloud?

  Quando gestisci risorse nel cloud, il provisioning e la gestione automatizzati delle risorse ti aiutano a gestire vari ambienti in modo efficiente. Gli strumenti APIs di automazione nativi variano a seconda dei provider di servizi cloud. Se possibile, prendi in considerazione l'utilizzo

di un set comune di strumenti di orchestrazione e distribuzione in grado di ospitare diverse risorse di provider di cloud. Ciò offre una maggiore flessibilità e semplifica le operazioni su più cloud. Tuttavia, potrebbe essere più semplice utilizzare l'automazione nativa di ciascun provider separatamente e stabilire processi organizzativi per garantire un utilizzo appropriato.

- Avete requisiti normativi e di conformità che ogni provider di servizi cloud deve soddisfare?

  Potresti avere considerazioni normative che determinano il modo in cui i dati devono essere archiviati e gestiti. Concentrati sulla standardizzazione delle politiche (come traffico di rete, archiviazione e sicurezza) che possono essere applicate automaticamente a ogni ambiente cloud tra i provider di cloud. Considerate in che modo le vostre applicazioni comunicheranno con i loro dati e li ospiteranno sullo stesso provider. Se le applicazioni e i relativi dati sono frammentati tra diversi provider, sarà difficile garantire il rispetto dei requisiti di conformità e normativi. Spesso è preferibile disporre delle applicazioni il più vicino possibile ai dati per ridurre al minimo la latenza di rete, massimizzare la velocità di trasmissione dei dati e limitare l'uscita dei dati, semplificando al contempo la sicurezza e i controlli di accesso.
- Sei in grado di ridurre al minimo il TCO e massimizzare gli sconti sui prezzi quando distribuisci applicazioni tra provider di cloud?

  È importante tenere conto del costo totale di proprietà (TCO) quando si considera il multicloud. L'esecuzione delle applicazioni su più provider cloud può aumentare i costi operativi e il sovraccarico amministrativo per mantenere e gestire le risorse in ogni ambiente. Inoltre, la diffusione dell'utilizzo tra più provider rende più difficile trarre vantaggio dagli sconti sui prezzi per volume o dagli accordi aziendali di uno specifico fornitore. Tieni conto di questi fattori quando stabilisci se i vantaggi del multicloud giustificano l'aumento del TCO.

Casi d'uso di esempio

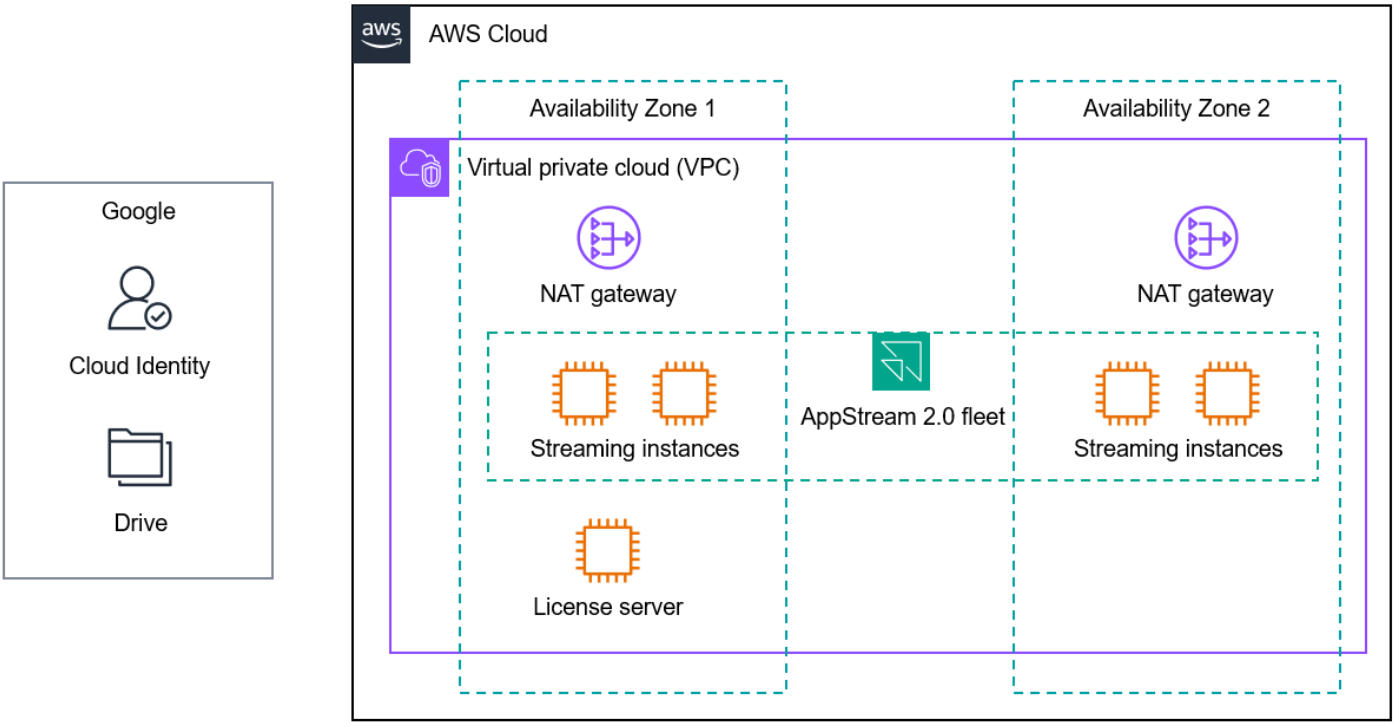
Per comprendere meglio l'applicazione di questi principi in diversi scenari, esaminiamo alcuni esempi di casi d'uso. Questi casi d'uso si basano sul modo in cui gli istituti di istruzione del mondo reale stanno adottando i servizi cloud.

- Laboratori informatici virtuali
- Previsione del successo degli studenti
- Federazione delle identità e Single Sign-On
- Cloud bursting per l'informatica di ricerca

Laboratori informatici virtuali

Nonostante la popolarità degli strumenti di apprendimento basati sul Web e l'abbondanza di dispositivi utente come laptop, Chromebook e tablet, la maggior parte degli istituti scolastici dispone di laboratori informatici fisici per applicazioni legacy o ad uso intensivo di risorse. Questi laboratori informatici sono spesso indispensabili per la scienza, la tecnologia, l'ingegneria e la matematica (STEM), l'istruzione professionale e tecnica (CTE), i media e l'arte, l'ingegneria e programmi simili. Le scuole possono ampliare o sostituire i laboratori informatici fisici con desktop virtuali basati sul cloud o servizi di streaming di applicazioni per garantire che tutti gli studenti abbiano accesso alle applicazioni di cui hanno bisogno in qualsiasi momento, da qualsiasi luogo e su qualsiasi dispositivo. Ciò migliora l'equità digitale, consente l'apprendimento remoto, garantisce un'esperienza utente coerente e protegge l'accesso remoto riducendo al contempo i costi.

Nell'istruzione primaria e secondaria (K12), molte scuole statunitensi utilizzano Amazon WorkSpaces Applications, un servizio di streaming di desktop e applicazioni completamente gestito, per fornire laboratori informatici virtuali che forniscono l'accesso ad Adobe Creative Cloud, al software Autodesk, ai programmi STEM e CTE come Project Lead the Way (PLTW) e altro ancora. Molte organizzazioni K12 gestiscono già il Single Sign-On e l'archiviazione dei file per studenti tramite Google Workspace e Google Drive, che sono applicazioni SaaS. Questi istituti possono configurare il single sign-on tra Google Workspace e Applications tramite la federazione SAML 2.0. WorkSpaces Possono anche configurare l'integrazione nativa tra WorkSpaces Applications e Google Drive in modo che gli studenti possano utilizzare lo spazio di archiviazione esistente. Il diagramma seguente illustra la distribuzione delle WorkSpaces applicazioni per questo caso d'uso.



Questa architettura segue questi consigli:

- Seleziona un provider cloud primario e strategico.Questa architettura utilizza i servizi cloud di un provider cloud principale. Sebbene includa l'integrazione con applicazioni SaaS che non sono ospitate sullo stesso provider, tali integrazioni vengono eseguite tramite semplici configurazioni. Le competenze e le competenze in materia di cloud sono necessarie solo per implementare e gestire i servizi del provider cloud principale.
- Distingui tra applicazioni SaaS e servizi cloud di base.Google Workspace e Google Drive non sono ospitati sullo stesso provider cloud della AppStream versione 2.0, ma ciò è accettabile perché questa implementazione fornisce le integrazioni necessarie. Il single sign-on consente la gestione centralizzata delle identità ed è configurato in modo sicuro tramite SAML 2.0. L'abilitazione dell'archiviazione cloud persistente per gli studenti richiede semplici modifiche alla configurazione in Google Drive e Applications. WorkSpaces
- Stabilisci i requisiti di sicurezza e governance per ogni provider di servizi cloud.I servizi e le integrazioni utilizzati in questa architettura aiutano a soddisfare i requisiti di sicurezza e governance di un istituto. Il traffico di streaming è crittografato. La federazione tramite Google Workspace consente la gestione centralizzata delle identità. I servizi di rete come Amazon Virtual Private Cloud (Amazon VPC) supportano la configurazione di sottoreti, routing e firewall. Puoi filtrare i contenuti utilizzando la configurazione DNS, gli agenti, le appliance virtuali o servizi gestiti come DNS

Firewall. Amazon Route 53 Resolver Puoi utilizzare servizi come quelli AWS Control Towerper garantire che l'account AWS che ospita WorkSpaces le applicazioni aderisca ai limiti e ai controlli organizzativi standard.

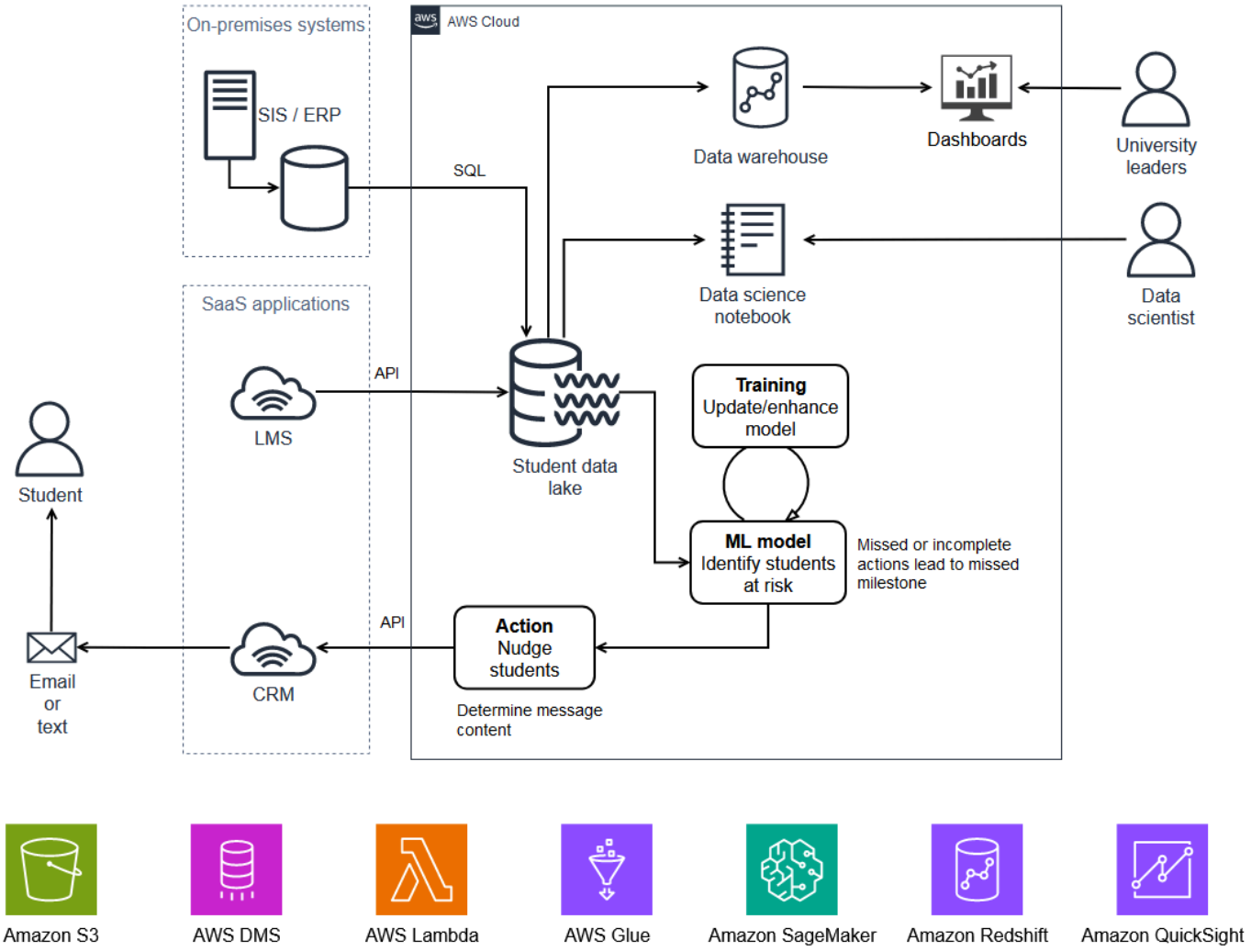
- Adotta soluzioni gestite native per il cloud laddove possibile e pratico. WorkSpaces Applications è un servizio gestito per lo streaming di desktop e applicazioni. È possibile eseguire lo streaming di desktop e applicazioni senza preoccuparsi del provisioning, del ridimensionamento o della manutenzione dei server. Installa le tue applicazioni, connetti le soluzioni di identità, rete e storage appropriate, quindi gestisci e trasmetti centralmente tali applicazioni agli utenti. In questo modo si elimina gran parte del carico di lavoro indifferenziato necessario per gestire una soluzione di streaming desktop virtuale personalizzata.

Previsione del successo degli studenti

Un'università del Midwest negli Stati Uniti ha scoperto che una manciata di attività chiave per gli studenti del primo anno in arrivo era altamente predittiva del successo, sia nel primo semestre di lezione dello studente che nel conseguimento della laurea. L'università voleva implementare un sistema che controllasse il completamento di queste attività e, quando si avvicinavano o superavano le scadenze chiave, voleva incoraggiare gli studenti a completare queste fasi.

I dati del sistema di gestione dell'apprendimento (LMS) SaaS sono stati un input chiave per questa soluzione, ma i dati si sono rivelati difficili da accedere ed elaborare con gli strumenti di data warehousing del team IT universitario. Inoltre, i messaggi agli studenti dovevano essere inviati tramite il sistema di gestione delle relazioni con i clienti (CRM) della scuola basato sul cloud. Per creare una soluzione funzionale e valutare l'efficacia dei suggerimenti agli studenti, l'università doveva avviare messaggi tramite il CRM e raccogliere dati da esso.

L'università ha sviluppato e implementato una soluzione in un unico ambiente cloud. La soluzione è una combinazione di servizi gestiti nativi del cloud, server cloud forniti e integrazioni con sistemi locali e applicazioni SaaS basate sul cloud. Come mostra il diagramma seguente, la soluzione inserisce i dati dal sistema informativo degli studenti (SIS), dall'LMS e dal CRM in un data lake. Utilizza questi dati per identificare gli studenti che rischiano di perdere attività chiave, invia loro messaggi tramite il CRM e fornisce una dashboard ai dirigenti universitari.



Questa architettura segue queste raccomandazioni:

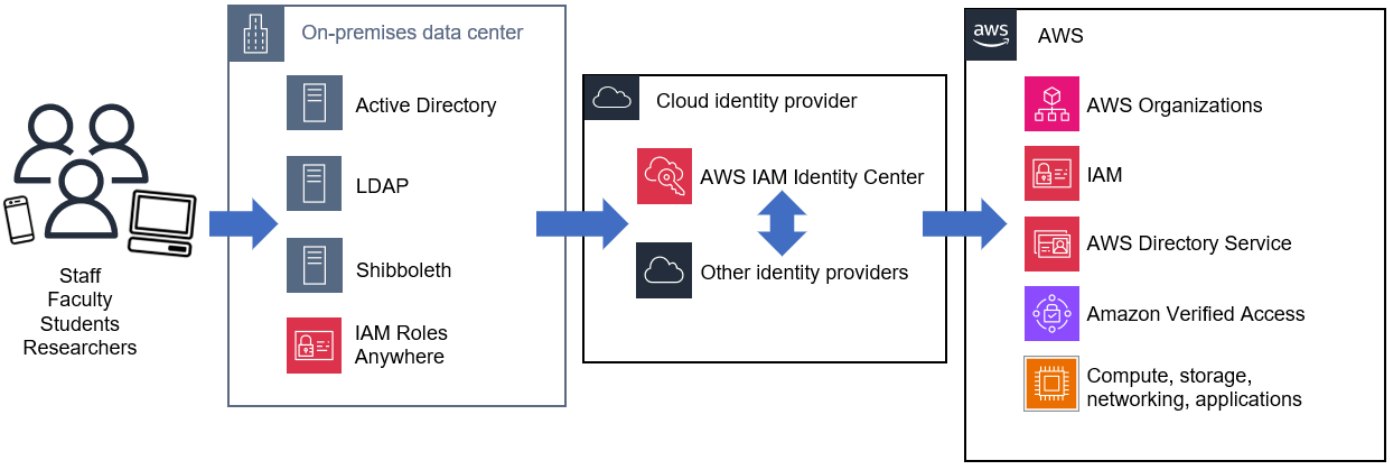
- Seleziona un provider cloud primario e strategico.Il provider cloud strategico dell'università ospita l'intera soluzione implementata. Ciò consente al personale IT e aziendale di concentrarsi sullo sviluppo di competenze in un unico set integrato di funzionalità cloud.
- Distingui tra applicazioni SaaS e servizi cloud di base.L'università distingue tra applicazioni SaaS e servizi di analisi cloud di base e utilizza integrazioni con le applicazioni SaaS per raccogliere dati e avviare le comunicazioni appropriate.
- Stabilisci i requisiti di sicurezza e governance per ogni provider di servizi cloud.L'università garantisce la sicurezza di tutti i componenti dell'architettura applicando barriere e controlli, inclusa la crittografia in transito e a riposo, per gestire i dati degli studenti in modo appropriato.

- Adotta soluzioni gestite native per il cloud laddove possibile e pratico.I servizi gestiti nativi del cloud vengono utilizzati per l'inserimento, l'archiviazione, il database e la funzionalità di estrazione, trasformazione e caricamento (ETL) dei dati, che riducono i tempi di sviluppo del flusso di lavoro di elaborazione dei dati. end-to-end

Federazione delle identità e Single Sign-On

Garantire una gestione coerente delle identità tra i sistemi principali è fondamentale per adottare con successo e in sicurezza qualsiasi tecnologia. Gli istituti scolastici adottano sempre più spesso soluzioni di identità e single sign-on basate sul cloud come AWS IAM Identity CenterMicrosoft Entra ID (precedentemente Azure Active Directory), Okta,,, Ping Identity, e CyberArk per semplificare la gestione delle identità JumpCloud OneLogin, ridurre il carico operativo e applicare centralmente le migliori pratiche come l'autenticazione a più fattori e l'accesso con privilegi minimi.

Molti di questi istituti mantengono ancora servizi di gestione delle identità e di directory come Active Directory e Shibboleth per i propri ambienti locali. Questi possono essere integrati con soluzioni basate sul cloud per consentire la gestione centralizzata delle identità e il single sign-on per studenti, docenti e personale. I fornitori di soluzioni cloud devono disporre di solide piattaforme di gestione delle easy-to-integrate identità che consentano di federare le identità tramite provider di identità cloud alle applicazioni esistenti, alle soluzioni SaaS e ai servizi cloud. Il diagramma seguente mostra un esempio di architettura.



Questa architettura segue questi consigli:

- Seleziona un provider cloud primario e strategico.Questa architettura viene utilizzata AWS come provider cloud principale. Integrandosi con un provider di identità cloud e i servizi di gestione delle

identità e di directory esistenti in locale, questa architettura supporta il provisioning e la gestione automatizzati dell'accesso sia ai servizi del provider cloud principale che ad altre applicazioni e soluzioni SaaS. Ciò garantisce che i requisiti di sicurezza e governance siano soddisfatti in modo coerente e facile da gestire man mano che ulteriori applicazioni e servizi vengono aggiunti al portafoglio tecnologico dell'istituto.

- Distingui tra applicazioni SaaS e servizi cloud di base.Questa architettura integra diversi tipi di sistemi di identità basati su cloud, SaaS e locali per fornire l'accesso a servizi e altre applicazioni. Cloud AWS Molti provider di identità basati su cloud e soluzioni Single Sign-On sono anche applicazioni SaaS e possono utilizzare integrazioni native e protocolli standard come SAML per funzionare in più ambienti.
- Stabilisci i requisiti di sicurezza e governance per ogni provider di servizi cloud.Questa architettura è conforme alle linee guida sulla gestione delle identità e degli accessi emesse da numerosi framework di sicurezza, tra cui il National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), NIST 800-171 e NIST 800-53. Le integrazioni con AWS Organizations, AWS Identity and Access Management (IAM) e altri servizi di AWS sicurezza, identità e conformità aiutano a fornire controlli di accesso sicuri e granulari basati sulle autorizzazioni di gruppo.
- Adotta servizi gestiti nativi per il cloud laddove possibile e pratico.Questa architettura utilizza servizi gestiti basati sul cloud per la gestione delle identità e il single sign-on. Ciò riduce il tempo e l'energia spesi per la gestione dell'infrastruttura e semplifica la manutenzione di questi sistemi critici.
- Implementa architetture ibride laddove esistenti, gli investimenti locali incentivano l'uso continuato.Questa architettura integra gli investimenti esistenti e locali nell'infrastruttura per l'hosting dei carichi di lavoro Active Directory, Lightweight Directory Access Control (LDAP) e Shibboleth e fornisce un percorso per spostare infine i principali servizi di identità in un'infrastruttura basata sul cloud. Inoltre, se i carichi di lavoro locali richiedono un accesso alle risorse basato su certificati, puoi utilizzare Roles Anywhere. AWSAWS Identity and Access Management

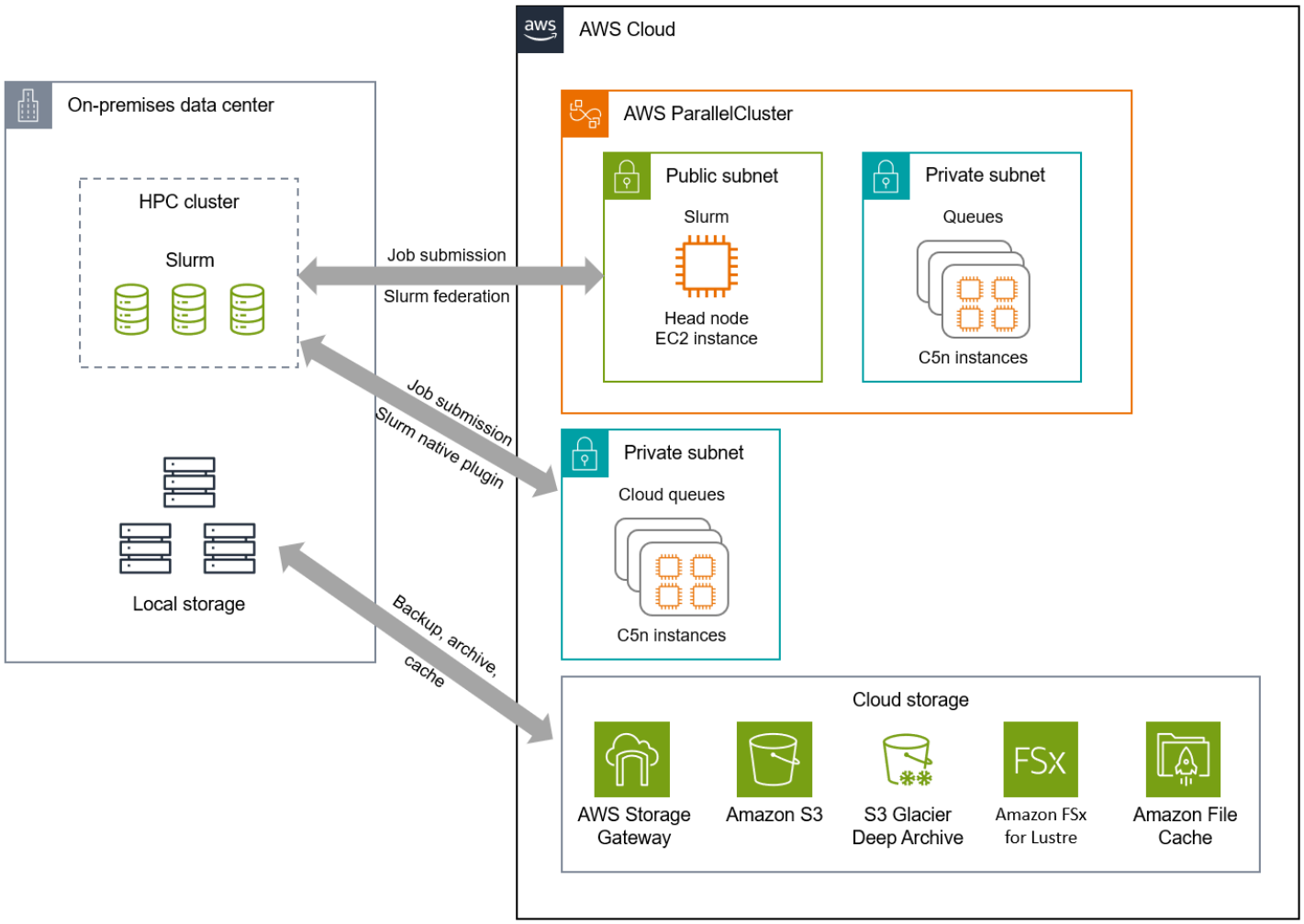
Cloud bursting per l'informatica di ricerca

Il gruppo di informatica di ricerca presso un istituto di ricerca R1 (Doctoral Universities — Very High Research Activity) negli Stati Uniti gestiva da molti anni cluster di calcolo ad alte prestazioni (HPC) locali con lo scheduler Slurm. Ad eccezione di alcune settimane di manutenzione programmata, i cluster funzionavano a un tasso di utilizzo dell'80-95% con la maggior parte delle code piene.

Il numero crescente di attività di ricerca presso l'istituto ha introdotto sfide in termini di capacità e capacità. Alcuni ricercatori di alto profilo eseguivano sempre simulazioni di lunga durata su determinate code, il che aumentava i tempi di attesa per gli altri utenti. I docenti appena assunti avevano bisogno di eseguire un gran numero di simulazioni meteorologiche per creare un nuovo modello di intelligenza artificiale e apprendimento automatico (AI/ML) per le previsioni meteorologiche, ma richiedevano una capacità maggiore di quella disponibile. Il gruppo informatico di ricerca stava inoltre ricevendo sempre più richieste per le più recenti unità di elaborazione grafica (GPUs) per addestrare modelli di apprendimento automatico. Anche se disponesse di nuovi fondi GPUs, il team avrebbe dovuto attendere mesi prima di ottenere l'approvazione per ampliare lo spazio su rack nel data center.

Molti ricercatori non erano disposti a eliminare i vecchi dati, quindi anche la capacità di archiviazione locale rappresentava una sfida. Era necessaria un'opzione di storage più scalabile e a lungo termine per liberare spazio di archiviazione prezioso e ad alte prestazioni in locale.

Il cloud affronta queste sfide con soluzioni di elaborazione e archiviazione ibride che consentono di trasferire l'informatica di ricerca nel cloud quando la capacità locale non è sufficiente. Il seguente diagramma di architettura illustra alcuni approcci che potenziano l'elaborazione e lo storage, utilizzando strumenti come e. AWS ParallelClusterGateway di archiviazione AWS



Questa architettura segue questi consigli:

- Seleziona un provider cloud primario e strategico.Questa architettura utilizza un provider cloud primario per evitare di essere limitata dall'approccio del minimo comune denominatore. In questo modo, l'istituto può trarre vantaggio dall'innovazione e dai servizi nativi di elaborazione e archiviazione offerti dal principale provider di servizi cloud. Il team di ricerca informatica può concentrarsi sull'ottimizzazione dei carichi di lavoro nell'ambiente fornito dal provider cloud principale, non su come lavorare in diversi ambienti cloud.
- Stabilisci i requisiti di sicurezza e governance per ogni provider di servizi cloud.Ogni servizio e strumento utilizzato in questa architettura può essere configurato per soddisfare i requisiti di sicurezza e governance del team di informatica di ricerca, tra cui connettività privata, crittografia dei dati in transito e a riposo, registrazione delle attività e altro ancora.
- Adotta servizi gestiti nativi del cloud laddove possibile e pratico.Questa architettura offre la possibilità di utilizzare servizi di storage ed elaborazione gestiti, nonché strumenti per semplificare

la gestione dei cluster. In questo modo, il team di ricerca informatica non deve preoccuparsi di gestire autonomamente i cluster o l'infrastruttura sottostante, operazione che può essere complessa e dispendiosa in termini di tempo.

- Implementa architetture ibride laddove esistenti, gli investimenti locali incentivano l'uso continuato.Questa architettura consente all'istituto di continuare a utilizzare le proprie risorse locali e di sfruttare il cloud per aumentare la capacità ed espandere la potenza di calcolo su richiesta. Con il cloud, l'istituto può dimensionare correttamente il tipo di elaborazione per massimizzare il rapporto prezzo/prestazioni e accedere alla tecnologia più recente per promuovere l'innovazione senza un grande investimento iniziale in hardware locale aggiuntivo.

Fasi successive

La scelta del modello di implementazione giusto per i carichi di lavoro cloud richiede un'attenta valutazione. Utilizza i consigli descritti in questo paper per guidare il processo decisionale ed evitare insidie comuni come complessità non necessaria, aumento della domanda di personale, governance incoerente e approcci con il minimo comune denominatore. Seguendo queste best practice, è possibile accelerare l'adozione del cloud per raggiungere e superare gli obiettivi istituzionali in modo più efficace.

Ricordati di selezionare un provider cloud primario e strategico e di istituire un Cloud Center of Excellence (CCoE) per promuovere la maturità organizzativa e garantire il tuo successo a lungo termine. Distingui tra applicazioni SaaS e servizi cloud di base e identifica i requisiti di sicurezza e governance principali per ciascuno di essi. Quando possibile, adotta servizi gestiti nativi del cloud e implementa architetture ibride quando gli investimenti esistenti nei data center incentivano l'uso continuato. Infine, prenota il multicloud solo per i carichi di lavoro che lo richiedono veramente.

AWS è ben posizionato per aiutarti a gestire ambienti singoli, ibridi e multicloud. Il tuo istituto può utilizzare soluzioni di AWS gestione e osservabilità come AWS Systems Managere Amazon CloudWatch per semplificare e centralizzare la gestione e il monitoraggio dell'infrastruttura e delle applicazioni, indipendentemente dall'ambiente. AWS Config Con servizi di dati e analisi come Amazon Athena e AWS GlueAWS DataSync, puoi ottenere informazioni dettagliate da tutti i tuoi dati, ovunque siano archiviati. Soluzioni ibride come AWS OutpostsAWS Wavelength, e AWS Snow Familyconsentono di portare AWS infrastrutture e servizi ovunque siano necessari. Strumenti come Amazon EKS Distro ti aiutano a creare cluster Kubernetes autogestiti su AWS, on-premise o su altri cloud.

Mentre definisci la tua strategia cloud, considera questi passaggi successivi:

1. Consulta il AWS Cloud Adoption Framework (AWS CAF) per identificare e assegnare priorità alle opportunità di trasformazione, valutare e migliorare la tua preparazione al cloud ed evolvere iterativamente la tua roadmap di trasformazione.
2. Identifica un sistema per l'implementazione del cloud da utilizzare come prova di fattibilità. Questo ti aiuterà a definire la base o il framework cloud per convalidare qualsiasi ipotesi e consentirà anche future implementazioni cloud.
3. Coinvolgi il team AWS del tuo account per discutere dei tuoi obiettivi di implementazione del cloud. Il team addetto all' AWS account può aiutarti a fornire chiarimenti, suggerire approcci,

identificare le dipendenze e anche collaborare con i team per tracciare il percorso dall'idea iniziale all'implementazione.

Collaboratori

I collaboratori di questa guida includono:

- Kevin Arand, Senior Manager, Architettura delle soluzioni, Istruzione, AWS
- Kevin McCandless, Senior Solutions Architect, K-12 Education, AWS
- Craig Jordan, Principal Solutions Architect, Istruzione, AWS
- Jesse Roberts, architetto principale delle soluzioni, SLG e K-12 Education, AWS
- Jianjun Xu, Principal Solutions Architect, Istruzione, AWS
- Josh Badal, Senior Solutions Architect, Istruzione, AWS
- Raj Chary, Architetto di soluzioni senior, Istruzione, AWS

Approfondimenti

Per ulteriori informazioni, fare riferimento a:

- AWS Centro di architettura
- Trasformazione del cloud nel settore pubblico
- AWS Framework di adozione del cloud (AWS CAF)
- AWS Soluzioni per ambienti ibridi e multicloud

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	—	15 settembre 2023

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:

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura 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 compatibile con Amazon Aurora PostgreSQL.
- 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 a 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 suMicrosoft 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

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.

funzione di aggregazione

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 AIOps viene utilizzata nella strategia di AWS migrazione, 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 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 interrompere 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.

implementazione blu/verde

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, vedere l'indicatore Implementate break-glass procedures nella guida Well-Architected AWS .

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 Cloud Adoption AWS Framework.

implementazione canaria

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

CCoE

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.

crittografia lato client

Crittografia dei dati a livello locale, prima che il destinatario li Servizio AWS riceva.

Centro di eccellenza 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 gli CCoE post 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 scalare l'adozione del cloud (ad esempio, creazione di una landing zone, definizione di una CCo E, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni
- Reinvenzione: ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post sul blog The Journey Toward Cloud-First & the Stages of Adoption on the Enterprise Strategy. Cloud AWS Per informazioni su come si relazionano alla 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 oBitbucket Cloud. Ogni versione del codice è denominata ramo. In una

struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola pipeline CI/CD 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 continua (continuous integration and continuous delivery, 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.

defense-in-depth

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 defense-in-depth approccio potrebbe combinare l'autenticazione a più fattori, la segmentazione della rete e la 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 Workloads 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 il modello del fico strangolatore (Strangler Fig), consulta la sezione Modernizzazione incrementale dei servizi Web Microsoft ASP.NET (ASMX) legacy utilizzando container e il Gateway Amazon API.

DOTT.

Vedi disaster recovery.

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, è possibile AWS CloudFormation utilizzarlo per rilevare deviazioni nelle risorse di sistema oppure AWS Control Tower per rilevare cambiamenti nella 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. I sistemi big-endian memorizzano per primo il byte più importante. I sistemi little-endian memorizzano per primo 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 epopee 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 in uno 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. I prompt con pochi passaggi 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 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. FMs sono in grado di svolgere 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.

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 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 alto livello che aiuta a governare le risorse, le politiche e la conformità tra le unità organizzative (). OUs 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 .

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 blocco

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.

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, come 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

IaC

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 in Well-Architected AWS Framework.

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. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs 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.

IIoInternet delle cose industriale (T)

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, vedere Creazione di una strategia di trasformazione digitale per l'Internet of Things (IIoT) industriale.

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPCs (nello stesso o in modo diverso Regioni AWS), Internet e le reti locali. La AWS Security Reference Architecture consiglia di configurare l'account di rete con informazioni in entrata, in uscita e di ispezione VPCs 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, vedere 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. LLMs

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.

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, consulta 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 machine-to-machine (M2M) leggero, basato sul modello di pubblicazione/sottoscrizione, per dispositivi IoT con risorse limitate.

microservizio

Un servizio piccolo e indipendente che comunica tramite canali ben definiti ed è in genere di proprietà di piccoli team autonomi. APIs 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 attraverso un'interfaccia ben definita utilizzando sistemi leggeri. APIs 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

Team interfunzionali 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 machine-to-machine (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 Well-Architected AWS Framework.

tecnologia operativa (OT)

Sistemi hardware e software che interagiscono con l'ambiente fisico per controllare le operazioni, le apparecchiature e le 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 tutti i bucket S3 in generale Regioni AWS, la crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche e dirette al bucket S3. `PUT` `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. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs 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`WHERE`. `true` `false`

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 di ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di sviluppo.

zone ospitate private

Un contenitore che contiene informazioni su come desideri che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più. VPCs 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 alle interruzioni o di ripristinarle. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud AWSPer 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 politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs 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.

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.

split-and-seed modello

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 Modernizzazione incrementale dei servizi Web legacy di Microsoft ASP.NET (ASMX) mediante container e Gateway Amazon API.

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

Coppie chiave-valore 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.

Transit Gateway

Un hub di transito di rete che puoi utilizzare per interconnettere le tue reti VPCs e quelle locali. 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 VPCs che consente di indirizzare il traffico utilizzando 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 query 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.