Best practice per semplificare l'osservabilità di Amazon EKS

# AWS Guida prescrittiva

# AWS Guida prescrittiva: Best practice per semplificare l'osservabilità di Amazon EKS

# Table of Contents

# Best practice per semplificare l'osservabilità di Amazon EKS

Ishwar Chauthaiwale, Naveen Suthar e Pratap Kumar Nanda, Amazon Web Services ()AWS

Marzo 2026 (storia del documento)

Amazon Elastic Kubernetes Service (Amazon EKS) richiede soluzioni di osservabilità complete per monitorare e risolvere efficacemente i carichi di lavoro containerizzati. I sistemi distribuiti e i microservizi hanno architetture complesse negli ambienti Amazon EKS, quindi l'implementazione di pratiche di osservabilità adeguate è fondamentale per mantenere operazioni affidabili. L'osservabilità efficace negli ambienti Amazon EKS consente ai team di ottenere informazioni approfondite sulle prestazioni delle applicazioni, risolvere i problemi in modo efficiente e mantenere lo stato ottimale del cluster.

La sfida consiste nel navigare nel vasto ecosistema di strumenti e tecniche disponibili per l'osservabilità di Amazon EKS, aderendo al contempo alle migliori pratiche in linea con gli obiettivi organizzativi e gli standard di settore. Le strategie di osservabilità efficaci devono bilanciare la raccolta completa dei dati con considerazioni sulle prestazioni, l'economicità e la scalabilità.

Questa guida è progettata per aiutare le organizzazioni a ottimizzare l'osservabilità di Amazon EKS nelle seguenti aree:

- Stabilire meccanismi di registrazione efficienti
- Implementazione di soluzioni di monitoraggio affidabili
- Utilizzo del tracciamento distribuito per architetture complesse
- Implementazione di strategie di allarme e risposta agli incidenti

Adottando queste best practice, la tua organizzazione può migliorare la propria capacità di acquisire informazioni approfondite sull'ambiente Amazon EKS, il che porta a una maggiore affidabilità, prestazioni ed efficienza operativa. Questo approccio semplificato all'osservabilità aiuta nella risoluzione dei problemi e nella manutenzione e supporta il processo decisionale basato sui dati per il miglioramento continuo delle applicazioni e dell'infrastruttura basate su Kubernetes. (Per informazioni dettagliate su Amazon EKS, consulta la documentazione del servizio.)

Questa guida approfondisce ogni aspetto dell'osservabilità di Amazon EKS ed esplora gli strumenti e le strategie che puoi personalizzare per soddisfare le esigenze specifiche delle tue implementazioni Amazon EKS, dalle applicazioni su piccola scala alle architetture di microservizi grandi e complesse.

In questa guida:



# Obiettivi

Questa guida può aiutare te e la tua organizzazione a raggiungere i seguenti obiettivi aziendali:

- Visibilità operativa migliorata: ottieni informazioni complete sui cluster e sulle applicazioni Amazon EKS attraverso pratiche di osservabilità efficaci.

  Questo obiettivo sottolinea l'importanza di mantenere una visibilità completa nell'ambiente Amazon EKS. Strumenti come AWS X-RayAmazon CloudWatch Container Insights e AWS Distro per OpenTelemetry aiutarti a comprendere il comportamento del sistema, identificare rapidamente i problemi e mantenere prestazioni ottimali.
- Migliore efficienza nella risoluzione dei problemi: riduci il tempo medio di rilevamento (MTTD) e il tempo medio di risoluzione (MTTR) attraverso strategie di tracciamento e monitoraggio efficaci.

  Questo obiettivo si concentra sull'implementazione di pratiche di osservabilità che consentano una rapida identificazione e risoluzione dei problemi. Tecniche come il tracciamento distribuito, la registrazione efficace e la raccolta completa delle metriche sono fondamentali per raggiungere questo obiettivo.
- Gestione proattiva delle prestazioni: consente l'individuazione precoce di potenziali problemi prima che si ripercuotano sugli utenti finali.

  Il monitoraggio proattivo è fondamentale per mantenere livelli elevati di disponibilità e prestazioni del servizio. Questo obiettivo risponde all'importanza di implementare avvisi adeguati, analisi delle tendenze e monitoraggio predittivo per prevenire interruzioni del servizio.
- Osservabilità conveniente: ottimizza i costi di osservabilità mantenendo al contempo una visibilità completa del sistema.

L'ottimizzazione dei costi comprende l'implementazione di strategie di campionamento efficienti, politiche di conservazione dei dati appropriate e approcci strumentali ottimali. L'obiettivo è bilanciare le esigenze di osservabilità con le considerazioni relative ai costi, garantendo al contempo un monitoraggio efficace del sistema.

- Architettura di monitoraggio scalabile: assicurati che le tue soluzioni di osservabilità si adattino perfettamente al tuo ambiente Amazon EKS.

  Questo obiettivo si concentra sull'implementazione di soluzioni di monitoraggio in grado di crescere con la tua applicazione. Indipendentemente dal fatto che stiate utilizzando un singolo cluster o una distribuzione multicluster e multiregione, la vostra strategia di osservabilità dovrebbe adattarsi di conseguenza

# Accesso ad Amazon EKS

La registrazione è un aspetto fondamentale della gestione e della manutenzione delle applicazioni eseguite su Amazon EKS. Le pratiche di registrazione efficaci negli ambienti Amazon EKS aiutano gli sviluppatori, i team operativi e gli amministratori di sistema a ottenere informazioni preziose sul comportamento, le prestazioni e lo stato delle loro applicazioni containerizzate e dell'infrastruttura sottostante.

L'implementazione di una solida strategia di registrazione in Amazon EKS è essenziale per diversi motivi:

- Risoluzione dei problemi: i log aiutano a identificare e diagnosticare rapidamente i problemi, riducendo i tempi di inattività e migliorando l'affidabilità complessiva del sistema.
- Conformità: molti settori richiedono una registrazione completa per scopi di controllo e regolamentazione.
- Sicurezza: l'analisi dei log può aiutarvi a rilevare e indagare su potenziali minacce o violazioni della sicurezza.
- Ottimizzazione delle prestazioni: i log forniscono informazioni dettagliate sulle prestazioni delle applicazioni e dei sistemi, in modo da identificare i punti deboli e ottimizzare l'utilizzo delle risorse.
- Monitoraggio e avvisi: i dati di registro possono essere utilizzati per configurare sistemi di monitoraggio e attivare avvisi per eventi o condizioni specifici.

In questa sezione:



## Tipi di registrazione in Amazon EKS

In Amazon EKS, la registrazione prevede l'acquisizione, l'archiviazione e l'analisi di vari tipi di dati di registro generati da diversi componenti del cluster Kubernetes, tra cui:

- Log di sistema: informazioni sulle istanze o sui nodi Amazon Elastic Compute Cloud (Amazon EC2) sottostanti AWS Fargate

- Log dei componenti Kubernetes: dati provenienti dai componenti principali di Kubernetes come il server API, lo scheduler e il controller manager
- Log di runtime del contenitore: informazioni dal runtime del contenitore, come Docker o containerd
- Log delle applicazioni: output da applicazioni containerizzate

Per gestire efficacemente i log nel tuo ambiente Amazon EKS, in genere utilizzi una combinazione di strumenti di Servizi AWS terze parti e best practice. Ciò potrebbe includere l'utilizzo di Amazon CloudWatch, Fluent Bit, Elasticsearch, Kibana e altri strumenti di registrazione e analisi per raccogliere, archiviare e visualizzare i dati di registro.

Le seguenti sezioni esplorano vari aspetti della registrazione in Amazon EKS, tra cui best practice, strumenti e tecniche per implementare una strategia di registrazione completa nei cluster Kubernetes su. AWS

## Registri di sistema

La registrazione per le istanze EC2 o i nodi Fargate sottostanti in Amazon EKS prevede approcci diversi a seconda del tipo di nodo.

Per implementare la registrazione per le istanze EC2 in Amazon EKS, puoi utilizzare i seguenti strumenti:

- CloudWatch agente: installa e configura l' CloudWatch agente sulle tue istanze EC2. Configuralo per raccogliere log di sistema come e. `/var/log/messages` `/var/log/secure` È possibile utilizzare script di dati utente o strumenti di gestione della configurazione per automatizzare questo processo.
- Fluent Bit: implementa Fluent Bit come strumento DaemonSet per raccogliere i log da tutti i nodi. Configuralo per inoltrare i log a Logs o ad altri sistemi di CloudWatch registrazione centralizzati.
- Container Insights: abilita Container Insights nel tuo cluster EKS per raccogliere automaticamente metriche e log dalle istanze EC2.
- Script personalizzati: sviluppa script personalizzati per raccogliere log specifici e inviarli alla destinazione di registrazione preferita.
- Agente SSM: utilizza Agent (SSM AWS Systems Manager Agent) per raccogliere e inoltrare i log ai log. CloudWatch

Per implementare la registrazione per i nodi Fargate in Amazon EKS, utilizza questi strumenti:

- Registrazione Fargate: Fargate raccoglie e registra automaticamente dai contenitori `stdout`. `stderr` Configura il tuo profilo Fargate per inviare questi log a Logs. CloudWatch
- Fluent Bit for Fargate AWS : fornisce un'immagine Fluent Bit specifica per la registrazione Fargate. Utilizzalo come contenitore laterale nei tuoi pod Fargate per raccogliere e inoltrare i registri.
- Container Insights for Fargate: abilita Container Insights per raccogliere metriche e log dai nodi Fargate.

## Registri dei componenti Kubernetes

La raccolta dei log dai componenti di Kubernetes come il server API, lo scheduler e il controller manager in Amazon EKS richiede un approccio leggermente diverso rispetto alla registrazione delle applicazioni. Questi componenti funzionano come parte del piano di controllo di Amazon EKS, gestito da AWS. Ecco come raccogliere e accedere a questi log:

- Abilita la registrazione del piano di controllo: puoi abilitare la registrazione del piano di controllo per il tuo cluster EKS tramite strumenti Console di gestione AWS, AWS Command Line Interface (AWS CLI) o Infrastructure as code (IaC) come Terraform. AWS CloudFormation Quando abiliti la registrazione del piano di controllo, i log vengono inviati ad Amazon CloudWatch Logs. Puoi visualizzarli nella CloudWatch console nel gruppo di log. `/aws/eks/<cluster-name>/cluster` All'interno di questo gruppo di log, ogni componente del piano di controllo ha il proprio flusso di log come segue:

| Nome dello stream | Description |
| --- | --- |
| server kube-api | Registri del server dell'API Kubernetes |
| kube-scheduler | Registri delle decisioni dello Scheduler |
| kube-controller-manager | Registri del gestore del controller |
| autenticatore | registri di autenticazione IAM |
| audit | Registri di controllo Kubernetes (devono essere abilitati in modo esplicito) |

  Per visualizzare i log di un componente specifico, vai al gruppo di log del cluster e filtra in base al nome del flusso di log di destinazione.

- Usa CloudWatch Logs Insights: puoi usare CloudWatch Logs Insights per eseguire query complesse sui tuoi log.
- Esportazione dei log su Amazon S3: per lo storage a lungo termine o per ulteriori analisi, puoi esportare i log in Amazon Simple Storage Service (Amazon S3).
- Utilizza strumenti di terze parti: puoi utilizzare strumenti come Fluent Bit per raccogliere questi log e inoltrarli ad altri sistemi di registrazione come Elasticsearch o Splunk.
- Utilizzo AWS CloudTrail: il AWS CloudTrailservizio può fornire ulteriori informazioni sulle chiamate API effettuate al cluster EKS.

## Registri di runtime del contenitore

La registrazione dei log di runtime dei container in Amazon EKS implica l'acquisizione e la gestione dei log dal runtime del contenitore, che in genere è per Amazon EKS. `containerd` Ecco come puoi affrontare la registrazione dei log di runtime dei container in Amazon EKS:

- Accedi direttamente ai log sui nodi Amazon EC2. Per i nodi EC2 autogestiti, puoi accedere direttamente ai log di runtime dei container sull'host da queste posizioni:
  - `containerd`registri: `/var/log/containers/`
  - Log Docker (se stai usando il runtime Docker): `/var/log/docker.log`
- Usa un file DaemonSet per la raccolta dei log.
- Implementa un agente di raccolta dei log (come Fluent Bit) DaemonSet per raccogliere i log da tutti i nodi.
- Configura l' CloudWatch agente per raccogliere i log di runtime dei contenitori.
- Abilita Container Insights per raccogliere le metriche e i log di runtime dei container.
- Usa Fargate. Per i nodi Fargate, i log di runtime dei container vengono raccolti automaticamente e sono accessibili tramite Logs. CloudWatch
- Implementa soluzioni di registrazione personalizzate utilizzando strumenti come Fluent Bit o Logstash. Imposta CloudWatchallarmi o usa strumenti come Prometheus per monitorare modelli o problemi specifici nei log di runtime dei container. Prendi in considerazione l'utilizzo di soluzioni di registrazione di terze parti che si integrano bene con Kubernetes e Amazon EKS, come Datadog, Splunk o Elastic Stack (ELK Stack). Utilizza gli strumenti di aggregazione dei log per raccogliere i log da più fonti e inoltrarli a un sistema di registrazione centralizzato.

## Log di applicazioni

I log delle applicazioni in Amazon EKS sono fondamentali per la manutenzione e la risoluzione dei problemi delle applicazioni. Per implementare la registrazione delle applicazioni in Amazon EKS, puoi scegliere tra queste opzioni:

- Scrivi i log sustdout/stderr: il modo più semplice e nativo di Kubernetes per gestire i log delle applicazioni consiste nel scriverli su and. `stdout` `stderr` Kubernetes acquisisce automaticamente questi flussi.
- Implementa l'aggregazione dei log: utilizza un aggregatore di log come Fluent Bit per raccogliere i log da tutti i tuoi pod.
- Configura il routing dei log: configura l'aggregatore di log per indirizzare i log verso la destinazione desiderata (come Logs o Elasticsearch). CloudWatch
- Usa CloudWatch Container Insights: abilita Container Insights per la registrazione e il monitoraggio completi.

# Le migliori pratiche per la registrazione in Amazon EKS

Le seguenti best practice aiutano a creare un sistema di registrazione robusto, scalabile ed efficiente per il tuo ambiente Amazon EKS e forniscono una migliore risoluzione dei problemi, il monitoraggio e la gestione complessiva dei tuoi cluster Kubernetes.

- Centralizza la raccolta dei log: utilizza una soluzione di registrazione centralizzata come CloudWatch Logs, Elasticsearch o un servizio di terze parti per aggregare i log di tutti i componenti. Ciò fornisce un unico punto di accesso per l'analisi dei log e semplifica la gestione.
- Implementa la registrazione strutturata: utilizza formati di log strutturati come JSON in modo che i log possano essere analizzati e ricercati più facilmente. Includi metadati pertinenti come timestamp, livelli di registro e identificatori di origine.
- Usa i livelli di registro in modo appropriato: implementa i livelli di registro appropriati (come`DEBUG`, `INFO` `WARN`, e`ERROR`) nelle tue applicazioni. Configura gli ambienti di produzione in modo che registrino i livelli appropriati per evitare un numero eccessivo di registrazioni.
- Abilita la registrazione dei container: configura i contenitori per accedere a `stdout` e. `stderr` Ciò consente a Kubernetes di acquisire e inoltrare questi log alla soluzione di registrazione prescelta.

- Abilita la registrazione delle applicazioni: configura le applicazioni per scrivere i log su `stdout` e `stderr` anziché scrivere nei file di registro. Ciò segue la metodologia delle app a 12 fattori e si allinea alle migliori pratiche native del cloud.
- Usa Kubernetes DaemonSets per la raccolta dei log: implementa agenti di raccolta dei log (come Fluent Bit) DaemonSets per assicurarti che vengano eseguiti su ogni nodo del cluster.
- Implementa politiche di conservazione: definisci e applica le politiche di conservazione dei log per rispettare le normative e gestire i costi di archiviazione.
- Dati di registro sicuri: crittografa i log in transito e a riposo. Implementa controlli di accesso per limitare chi può visualizzare e gestire i log.
- Monitora l'inserimento dei log: imposta avvisi per errori o ritardi nell'inserimento dei log per garantire la registrazione continua.
- Usa annotazioni ed etichette Kubernetes: utilizza le annotazioni e le etichette Kubernetes per aggiungere metadati ai log, per migliorare la ricercabilità e il filtraggio.
- Implementa il tracciamento distribuito: utilizza strumenti di tracciamento distribuito come o Jaeger per correlare i log tra i microservizi. AWS X-Ray
- Ottimizza il volume dei log: sii selettivo su ciò che registri per evitare costi inutili e problemi di prestazioni. Utilizza il campionamento per log ad alto volume e di basso valore.
- Implementa l'aggregazione dei log: utilizza strumenti come Logstash per aggregare i log provenienti da più fonti prima di inviarli al sistema di registrazione centrale.
- Utilizza Servizi AWS quando possibile: servizi come CloudWatch Logs e Container Insights offrono una perfetta integrazione con altri. Servizi AWS
- Implementa l'analisi e la visualizzazione dei log: utilizza strumenti come CloudWatch Logs Insights, Elasticsearch con Kibana o soluzioni di terze parti per l'analisi e la visualizzazione dei log.
- Implementa l'analisi automatizzata dei log: utilizza strumenti di apprendimento automatico e basati sull'intelligenza artificiale per rilevare automaticamente anomalie e modelli nei log.
- Documenta la tua strategia di registrazione: mantieni una documentazione chiara dell'architettura, delle pratiche e degli strumenti di registrazione per il tuo team.

## Considerazioni importanti per la registrazione in Amazon EKS

Questa sezione illustra importanti considerazioni da tenere a mente quando si implementa la registrazione in Amazon EKS.

- Impatto sulle prestazioni: una registrazione eccessiva può influire sulle prestazioni dell'applicazione. Prestate attenzione al volume e alla frequenza dei log generati.
- Gestione dei costi: l'archiviazione e l'elaborazione dei log possono comportare costi significativi, soprattutto su larga scala. Implementa politiche di conservazione dei log e valuta la possibilità di utilizzare l'aggregazione dei log per ridurre i costi.
- Sicurezza e conformità: assicurati che i log non contengano informazioni sensibili come password o dati personali. Implementa la crittografia per i log in transito e a riposo. Prendi in considerazione requisiti di conformità come il Regolamento generale sulla protezione dei dati (GDPR) o l'Health Insurance Portability and Accountability Act (HIPAA) quando gestisci i log.
- Scalabilità: assicurati che la tua soluzione di registrazione sia scalabile in base alle dimensioni del cluster e al volume di log. Prendi in considerazione l'utilizzo del buffering e del batching per la trasmissione dei log.
- Conservazione dei log: definisci e implementa periodi di conservazione dei log appropriati. Bilancia i requisiti di conformità con i costi di storage.
- Controllo degli accessi: implementa ruoli e policy AWS Identity and Access Management (IAM) adeguati per l'accesso ai log. Segui il principio del privilegio minimo per la gestione dei log.
- Coerenza dei log: utilizza formati di registro coerenti tra diverse applicazioni e servizi. Utilizza la registrazione strutturata per semplificare l'analisi e l'analisi.
- Sincronizzazione dell'ora: sincronizza l'ora su tutti i nodi per ottenere timestamp coerenti nei log.
- Allocazione delle risorse: alloca le risorse appropriate (come CPU e memoria) per gli agenti di registrazione. Monitora l'utilizzo delle risorse dei componenti di registrazione.
- Considerazioni su Fargate: Fargate dispone di meccanismi di registrazione specifici che differiscono dai nodi basati su EC2. Comprendi i limiti e le funzionalità della registrazione Fargate.
- Cluster multi-tenant: negli ambienti multi-tenant, assicuratevi che i log siano isolati correttamente tra i tenant.
- Analisi e analisi dei log: considera gli strumenti e le competenze necessari per un'analisi efficace dei log. Implementa l'analisi dei log per l'estrazione strutturata dei dati.
- Monitoraggio del sistema di registrazione: imposta il monitoraggio per l'infrastruttura di registrazione stessa. Genera avvisi per la registrazione di errori o arretrati del sistema.
- Impatto sulla rete: fate attenzione alla larghezza di banda di rete utilizzata dalla trasmissione dei log. Prendi in considerazione l'utilizzo della compressione per i dati di registro.
- Eventi Kubernetes: non trascurare gli eventi Kubernetes come fonte di informazioni importanti.

- Registrazione del piano di controllo: comprendi le implicazioni e i costi dell'abilitazione della registrazione del piano di controllo.
- Funzionalità di debug: assicurati che la tua soluzione di registrazione consenta di eseguire facilmente il debug e la risoluzione dei problemi.
- Integrazione con gli strumenti esistenti: valuta in che modo la tua soluzione di registrazione Amazon EKS si integra con gli strumenti di monitoraggio e avviso esistenti.
- Test: verifica regolarmente la configurazione di registrazione, soprattutto dopo gli aggiornamenti del cluster.
- Documentazione: mantieni una documentazione chiara dell'architettura e delle pratiche di registrazione.
- Latenza di aggregazione dei log: fai attenzione a qualsiasi latenza nell'aggregazione dei log e a come potrebbe influire sul monitoraggio in tempo reale.

# Monitoraggio in Amazon EKS

Il monitoraggio in Amazon EKS offre una visibilità fondamentale sullo stato, le prestazioni e la sicurezza dei carichi di lavoro Kubernetes. Senza un monitoraggio adeguato, si rischiano interruzioni del servizio, violazioni della sicurezza e un utilizzo inefficiente delle risorse che possono influire sulle operazioni aziendali e aumentare i costi. Un monitoraggio efficace consente di identificare e risolvere in modo proattivo i problemi, ottimizzare l'utilizzo delle risorse e mantenere i requisiti di conformità nelle applicazioni containerizzate. Implementando soluzioni di monitoraggio complete, puoi garantire un'elevata disponibilità, rilevare tempestivamente le anomalie e prendere decisioni basate sui dati per scalare e migliorare la tua infrastruttura Amazon EKS.

Questa sezione esplora i vari aspetti del monitoraggio di Amazon EKS, inclusi diversi tipi di monitoraggio, strumenti disponibili e best practice per aiutarti a creare una solida strategia di monitoraggio per il tuo ambiente Kubernetes.

In questa sezione:



# Tipi di monitoraggio in Amazon EKS

L'osservabilità efficace in Amazon EKS implica attività di monitoraggio dell'infrastruttura, delle applicazioni e della sicurezza.

## Monitoraggio dell'infrastruttura

Il monitoraggio dell'infrastruttura è un componente fondamentale dell'osservabilità di Amazon EKS che fornisce informazioni approfondite sullo stato e le prestazioni degli elementi fondamentali del cluster Kubernetes. Fondamentalmente, consiste nel tracciare i segni vitali dei componenti del piano di controllo e dei nodi di lavoro e garantire che la piattaforma sottostante rimanga stabile ed efficiente.

- Il monitoraggio del piano di controllo è fondamentale perché supervisiona componenti chiave come il server API, il database etcd e lo scheduler. Monitorando la latenza del server API, è possibile

identificare rapidamente i rallentamenti prestazionali che potrebbero influire sulla distribuzione delle applicazioni o sulle operazioni di scalabilità. Il monitoraggio delle prestazioni di Etcd verifica che il database di stato del cluster funzioni in modo efficiente e previene problemi di coerenza dei dati che potrebbero influire sull'intero cluster.

- Il monitoraggio a livello di nodo è altrettanto importante perché si concentra sulle risorse di calcolo che eseguono i carichi di lavoro containerizzati. Ciò include il monitoraggio dell'utilizzo della CPU, del consumo di memoria, dell'I/O del disco e delle prestazioni di rete su tutti i nodi di lavoro. La comprensione di queste metriche aiuta a prevenire l'esaurimento delle risorse, a ottimizzare le decisioni sulla scalabilità dei nodi e a garantire un'adeguata pianificazione della capacità.
- Il monitoraggio della rete svolge un ruolo fondamentale nel mantenere una comunicazione affidabile tra pod, servizi e risorse esterne. Monitorando la velocità effettiva, la latenza e gli stati di connessione della rete, è possibile identificare tempestivamente i problemi di connettività e garantire una comunicazione fluida delle applicazioni. Il monitoraggio dello storage integra il monitoraggio della rete monitorando i volumi, le prestazioni, l'utilizzo della capacità e i I/O modelli, per aiutare a prevenire i colli di bottiglia legati ai dati.

Il monitoraggio dell'infrastruttura funge da sistema di allarme rapido per potenziali problemi, consente una manutenzione proattiva e garantisce un'allocazione ottimale delle risorse. Senza un solido monitoraggio dell'infrastruttura, si rischiano tempi di inattività imprevisti, prestazioni ridotte e utilizzo inefficiente delle risorse che possono avere un impatto significativo sulle operazioni e sui costi aziendali.

## Monitoraggio dell'applicazione

Il monitoraggio delle applicazioni è essenziale per mantenere applicazioni containerizzate sane, performanti e affidabili nel tuo ambiente Amazon EKS. Questo livello di monitoraggio si concentra sui carichi di lavoro effettivi eseguiti all'interno del cluster e fornisce informazioni fondamentali su come le applicazioni si comportano, si comportano e interagiscono con altri servizi.

Il monitoraggio delle applicazioni include il monitoraggio a livello di contenitore, il monitoraggio a livello di servizio e la traccia distribuita.

- A livello di container, il monitoraggio delle applicazioni tiene traccia di parametri cruciali come lo stato di salute dei container, il numero di riavvii e i modelli di consumo delle risorse. Queste metriche aiutano a identificare i contenitori problematici che potrebbero consumare risorse eccessive o subire riavvii frequenti, il che potrebbe indicare problemi di fondo come perdite di memoria o problemi di configurazione. Monitorando gli eventi del ciclo di vita dei container, è

possibile garantire il corretto comportamento delle applicazioni e risolvere rapidamente i problemi di distribuzione.

- Il monitoraggio a livello di servizio offre visibilità sulle metriche relative alle prestazioni e all'affidabilità delle applicazioni, come i tempi di risposta, i tassi di errore e il throughput delle richieste. Queste metriche sono fondamentali per mantenere gli obiettivi a livello di servizio (SLOs) e garantire un'esperienza positiva per l'utente finale. È possibile tenere traccia della latenza tra diversi endpoint di servizio, identificare i punti deboli nelle prestazioni e monitorare i modelli di errore per mantenere l'affidabilità delle applicazioni.
- Il tracciamento distribuito è un altro aspetto fondamentale del monitoraggio delle applicazioni, in particolare nelle architetture di microservizi. Implementando il tracciamento, è possibile seguire le richieste mentre fluiscono attraverso diversi servizi, comprendere le dipendenze e identificare i punti deboli in termini di prestazioni. Questa end-to-end visibilità consente di ottimizzare le interazioni con i servizi e risolvere problemi complessi che riguardano più componenti.

Le metriche applicative personalizzate svolgono un ruolo cruciale nel fornire informazioni specifiche per l'azienda. Queste potrebbero includere metriche come i tassi di elaborazione degli ordini, le frequenze di accesso degli utenti o le percentuali di successo delle transazioni. È possibile correlare queste metriche personalizzate con le metriche dell'infrastruttura e dei container per comprendere meglio in che modo le prestazioni dell'infrastruttura influiscono sulle operazioni aziendali e prendere decisioni basate sui dati per la scalabilità e l'ottimizzazione.

L'importanza del monitoraggio delle applicazioni risiede nella sua capacità di fornire una visione completa dello stato e delle prestazioni delle applicazioni. Questo monitoraggio consente di mantenere un'elevata qualità del servizio, risolvere rapidamente i problemi e ottimizzare continuamente le applicazioni per raggiungere gli obiettivi aziendali.

## Controllo della sicurezza

Il monitoraggio della sicurezza in Amazon EKS è un'attività fondamentale che aiuta le organizzazioni a mantenere l'integrità, la riservatezza e la conformità dei loro ambienti Kubernetes. Questo approccio di sicurezza completo combina sorveglianza continua, rilevamento delle minacce e monitoraggio della conformità per proteggere i carichi di lavoro containerizzati da potenziali rischi per la sicurezza e accessi non autorizzati. Include il monitoraggio dell'autenticazione e delle autorizzazioni, il monitoraggio della sicurezza della rete e il monitoraggio della configurazione e della conformità.

- Il monitoraggio dell'autenticazione e delle autorizzazioni costituisce la prima linea di difesa poiché tiene traccia di tutti i tentativi di accesso al cluster. Ciò include il monitoraggio delle richieste del server API, il monitoraggio dei tentativi di accesso riusciti e falliti e il controllo delle modifiche al controllo degli accessi basato sui ruoli (RBAC). Conservando registri di controllo dettagliati su chi ha avuto accesso a quali risorse e quando, è possibile rilevare rapidamente potenziali violazioni della sicurezza, tentativi di accesso non autorizzati o attività di escalation dei privilegi. Ciò è particolarmente importante negli ambienti multi-tenant in cui è essenziale mantenere rigorosi controlli di accesso.
- Il monitoraggio della sicurezza della rete si concentra sul rilevamento e la prevenzione delle comunicazioni non autorizzate tra pod e servizi. Monitorando le violazioni delle policy di rete e gli schemi di traffico insoliti, è possibile identificare potenziali minacce alla sicurezza, come i tentativi di fuga dei container o i movimenti laterali all'interno del cluster. Ciò include il monitoraggio sia delle comunicazioni interne del cluster che dei modelli di traffico esterno per garantire che i container comunichino solo con gli endpoint autorizzati e seguano le politiche di sicurezza definite.
- Il monitoraggio della configurazione e della conformità è essenziale per mantenere le linee di base di sicurezza e soddisfare i requisiti normativi. Implica la scansione continua delle immagini dei container alla ricerca di vulnerabilità, il monitoraggio della sicurezza in fase di esecuzione e il monitoraggio delle modifiche alla configurazione che potrebbero influire sul livello di sicurezza. I controlli di conformità regolari garantiscono il rispetto degli standard di settore e delle politiche di sicurezza organizzative, mentre il rilevamento delle deviazioni nella configurazione aiuta a prevenire modifiche non autorizzate che potrebbero introdurre rischi per la sicurezza.

Il monitoraggio della sicurezza in Amazon EKS offre la visibilità e il controllo necessari per proteggere dalle moderne minacce alla sicurezza, garantendo al contempo la conformità ai requisiti normativi. Implementando un monitoraggio completo della sicurezza, la tua organizzazione può mantenere un solido livello di sicurezza, rispondere rapidamente agli incidenti di sicurezza e dimostrare la conformità a vari standard normativi.

# Strumenti di monitoraggio per Amazon EKS

Questa sezione illustra tre categorie di strumenti di monitoraggio Amazon EKS: servizi di AWS monitoraggio, soluzioni open source o proprietarie e strumenti specializzati.

## AWS servizi

- Amazon CloudWatch: servizio completo di monitoraggio e registrazione

CloudWatch costituisce la spina dorsale delle soluzioni di AWS monitoraggio e offre funzionalità estese per gli ambienti Amazon EKS. Fornisce Container Insights per metriche granulari di container e cluster, in modo da poter monitorare le prestazioni, l'utilizzo delle risorse e lo stato delle applicazioni. Il servizio eccelle nell'aggregazione e nell'analisi dei log e supporta la registrazione centralizzata su contenitori e nodi. CloudWatch si integra naturalmente con. Servizi AWS Fornisce una configurazione automatica degli allarmi e supporta parametri e dashboard personalizzati, che lo rendono uno strumento essenziale per il monitoraggio di Amazon EKS.

- AWS X-Ray: Piattaforma di tracciamento distribuita avanzata

  X-Ray aumenta l'osservabilità fornendo sofisticate funzionalità di tracciamento distribuito. La visualizzazione della mappa dei servizi offre informazioni chiare sull'architettura e sulle dipendenze delle applicazioni, mentre il monitoraggio dettagliato delle richieste aiuta a identificare i punti deboli delle prestazioni tra i servizi. X-Ray è in grado di tracciare le richieste attraverso architetture di microservizi complesse, il che lo rende prezioso per la risoluzione dei problemi e l'ottimizzazione, specialmente nei sistemi distribuiti che si estendono su più piattaforme. Servizi AWS

- AWS Distro per: framework di osservabilità unificato OpenTelemetry

  Distro for OpenTelemetry offre funzionalità di raccolta dati unificate con supporto multipiattaforma, il che lo rende ideale per ambienti ibridi. Questo servizio si integra con altri Servizi AWS, supporta strumentazione personalizzata e offre flessibilità nell'implementazione di soluzioni di monitoraggio complete pur mantenendo la compatibilità con gli standard del settore.

- Amazon Managed Grafana: visualizzazione di livello aziendale

  Amazon Managed Grafana fornisce un servizio completamente gestito per la visualizzazione e l'analisi dei dati. Offre una perfetta integrazione con altre Servizi AWS funzionalità di sicurezza integrate e una scalabilità di livello aziendale. Il servizio semplifica la creazione e la gestione di dashboard fornendo al contempo funzionalità avanzate come l'accesso alla fonte di dati tra account e l'integrazione con. AWS IAM Identity Center

- Amazon Managed Service for Prometheus: monitoraggio gestito, sicuro e ad alta disponibilità

  Amazon Managed Service for Prometheus è un servizio di monitoraggio completamente gestito e compatibile con Prometheus. Fornisce scalabilità automatizzata, elevata disponibilità e acquisizione e interrogazione sicure delle metriche. Il servizio si integra perfettamente con Amazon EKS ed elimina il sovraccarico operativo della gestione dei server Prometheus.

## Soluzioni open source o proprietarie

Gli AWS strumenti descritti nella sezione precedente offrono una perfetta integrazione e servizi gestiti. Gli strumenti open source elencati in questa sezione si completano Servizi AWS offrendo flessibilità e ampie opzioni di personalizzazione. Comprendere le funzionalità e i casi d'uso di ogni strumento consente di progettare strategie di monitoraggio che soddisfino al meglio i requisiti specifici.

- Prometheus: toolkit per la raccolta di metriche

  Prometheus è una soluzione open source per la raccolta di metriche in ambienti Kubernetes. Il suo database di serie temporali e il linguaggio di query PromQL consentono analisi metriche sofisticate. Le funzionalità di rilevamento dei servizi della piattaforma si adattano automaticamente agli ambienti Kubernetes dinamici e il suo sistema di gestione degli avvisi ti tiene informato sulle questioni critiche. Prometheus offre ampie opzioni di integrazione, che lo rendono una scelta versatile per il monitoraggio completo delle metriche.

- Grafana: motore di visualizzazione avanzato

  Grafana trasforma dati di monitoraggio complessi in informazioni fruibili attraverso le sue funzionalità di visualizzazione. La piattaforma crea dashboard personalizzate che combinano dati provenienti da più fonti e forniscono una visione unificata delle metriche dell'infrastruttura e delle applicazioni. Il supporto per varie fonti di dati e le funzionalità di gestione degli avvisi forniscono un monitoraggio completo. Grafana può aiutarti a visualizzare dati storici e in tempo reale, in modo da identificare le tendenze e prendere decisioni informate.

- Fluent Bit: livello di registrazione unificato

  Questa soluzione di registrazione fornisce la raccolta e la gestione dei log per gli ambienti Kubernetes. La sua integrazione nativa con Kubernetes garantisce una raccolta di log senza interruzioni da contenitori e nodi e il supporto per più destinazioni di output offre flessibilità nell'archiviazione e nell'analisi dei log. Funzionalità avanzate come l'analisi e il filtraggio dei log consentono di elaborare e indirizzare i log in base a requisiti specifici. La natura leggera di Fluent Bit lo rende particolarmente adatto per ambienti containerizzati.

- Datadog: osservabilità completa

  Datadog offre funzionalità di monitoraggio complete con supporto nativo di Kubernetes. Offre monitoraggio dell'infrastruttura, monitoraggio delle prestazioni delle applicazioni (APM), gestione dei log e analisi in tempo reale. Puoi utilizzare il rilevamento automatico dei servizi e l'ampio

catalogo di integrazione della piattaforma per il monitoraggio di Amazon EKS e le sue funzionalità di apprendimento automatico per rilevare anomalie e prevedere potenziali problemi.

- New Relic: monitoraggio delle prestazioni delle applicazioni

  New Relic offre visibilità sulle prestazioni delle applicazioni e sullo stato dell'infrastruttura. La sua integrazione con Kubernetes fornisce informazioni dettagliate sui container, tracciamento distribuito e dashboard personalizzati. La piattaforma consente di correlare le prestazioni delle applicazioni con i parametri dell'infrastruttura, in modo da identificare e risolvere rapidamente i problemi.

- Elastic Stack (ELK Stack): analisi e ricerca dei log

  ELK Stack combina Elasticsearch, Logstash e Kibana per fornire funzionalità di gestione e analisi dei log. Offre funzionalità di ricerca avanzate, strumenti di visualizzazione e funzionalità di apprendimento automatico. Puoi utilizzare lo stack per gestire grandi volumi di dati di log dai tuoi ambienti Amazon EKS.

## Strumenti specializzati

È possibile combinare i seguenti strumenti in base ai requisiti di monitoraggio specifici, alla scala delle operazioni e alle preferenze organizzative. La chiave è creare uno stack di monitoraggio che offra una visibilità completa pur rimanendo gestibile ed economico.

- kube-state-metrics (KSM): monitoraggio dello stato di Kubernetes

  Questo servizio aggiuntivo ascolta il server API Kubernetes e genera metriche sullo stato degli oggetti. Fornisce informazioni sullo stato di integrità delle implementazioni, dei pod e di altre risorse Kubernetes.

- Kubernetes Metrics Server: metriche delle risorse

  Questo server di metriche raccoglie le metriche delle risorse da Kubelets e le espone tramite l'API Kubernetes Metrics. Fornisce la scalabilità automatica dei pod orizzontali e metriche di base di CPU e memoria.

- Kubecost: monitoraggio dei costi di Kubernetes

  Strumenti come Kubecost forniscono analisi dettagliate dei costi e consigli di ottimizzazione per i cluster EKS. Ti aiutano a comprendere e ottimizzare la spesa per il cloud su diversi namespace, implementazioni e servizi.

# Implementazione dell'alta disponibilità per le soluzioni di monitoraggio Amazon EKS

Una solida strategia di alta disponibilità (HA) per il monitoraggio di Amazon EKS è fondamentale per garantire una visibilità continua nel tuo ambiente Kubernetes. Questa sezione illustra un approccio completo all'implementazione dell'HA in diversi aspetti dell'infrastruttura di monitoraggio.

## Ridondanza e scalabilità dell'architettura

La creazione di un sistema di monitoraggio ad alta disponibilità inizia con una corretta progettazione architettonica. I componenti di monitoraggio devono essere distribuiti su più zone di AWS disponibilità per proteggere dai guasti delle zone. Ciò include l'implementazione della scalabilità orizzontale per componenti di monitoraggio critici come server Prometheus, log collector e gestori di avvisi. Puoi utilizzare servizi AWS gestiti come Amazon Managed Service for Prometheus e Amazon Managed Grafana per ridurre il sovraccarico operativo garantendo al contempo un'elevata disponibilità. Configura meccanismi di failover automatici per mantenere la continuità del servizio durante i guasti dei componenti, implementando controlli dello stato e procedure di ripristino automatizzate.

## Strategia di archiviazione dei dati resiliente

La resilienza dell'archiviazione dei dati è fondamentale per mantenere l'affidabilità del sistema di monitoraggio. L'implementazione di soluzioni di storage distribuite garantisce che i dati e i log metrici rimangano accessibili anche in caso di guasto dei singoli nodi di storage. Ciò include la configurazione della corretta replica dei dati su più zone di disponibilità e l'utilizzo di diversi backend di storage per la ridondanza. Stabilisci procedure di backup regolari per i dati storici, con processi di ripristino documentati per vari scenari di errore. Per i database di serie temporali come Prometheus, l'implementazione di soluzioni di storage remoto aiuta a separare i problemi di archiviazione dalla raccolta dei dati e migliora l'affidabilità complessiva del sistema.

## Gestione ridondante degli avvisi

La gestione degli avvisi richiede un'attenzione speciale in una configurazione HA. L'implementazione di gestori di avvisi ridondanti garantisce che le notifiche critiche raggiungano i destinatari previsti anche in caso di guasti del sistema. Configura più canali di notifica come e-mail, SMS, Slack e PagerDuty fornisci percorsi di comunicazione alternativi. Utilizza meccanismi di deduplicazione degli avvisi per prevenire tempeste di avvisi durante guasti parziali del sistema e metodi di notifica fallback per garantire che gli avvisi critici non vengano mai persi. L'implementazione della correlazione degli

avvisi aiuta a mantenere il contesto durante gli scenari di failover e previene la duplicazione delle notifiche provenienti da sistemi ridondanti.

## Bilanciamento del carico e individuazione dei servizi

Un corretto bilanciamento del carico è essenziale per mantenere stabili i servizi di monitoraggio. AWS Gli Application Load Balancer distribuiscono il traffico di monitoraggio in entrata su più endpoint e i controlli di integrità assicurano che il traffico venga indirizzato solo verso istanze integre. I meccanismi di rilevamento dei servizi aiutano i componenti di monitoraggio ad adattarsi automaticamente ai cambiamenti dell'ambiente, come l'aggiunta di nuovi nodi o servizi. Implementa gli agenti di monitoraggio in modo coerente su tutti i nodi utilizzandoli DaemonSets per garantire una copertura completa man mano che il cluster cresce.

## Considerazioni aggiuntive sull'HA

Resilienza della rete:

- Implementa percorsi di rete ridondanti.
- Configura la corretta progettazione della sottorete tra le zone di disponibilità.
- Utilizzare AWS Direct Connectcon percorsi di backup.
- Configura i gruppi di sicurezza e gli elenchi di controllo degli accessi alla rete appropriati (rete ACLs).

Monitoraggio dei monitor:

- Implementa sistemi di monitoraggio secondari.
- Implementa il monitoraggio interregionale.
- Configura gli avvisi per i sistemi che non rispondono.
- Verifica regolarmente le procedure di failover.

Pianificazione della capacità:

- Monitora le tendenze di utilizzo delle risorse.
- Implementa la scalabilità predittiva.
- Verifica regolarmente le prestazioni.

Gestione dei dati:

- Implementare politiche di conservazione dei dati.
- Configura l'aggregazione delle metriche.
- Pianifica la gestione del ciclo di vita dei dati.
- Ottimizza lo storage su base regolare.

Procedure di ripristino:

- Processi di recupero dei documenti.
- Testa regolarmente il disaster recovery.
- Implementa il ripristino automatico ove possibile.
- Identifica e implementa percorsi di escalation chiari.

Implementando queste pratiche di alta disponibilità, puoi garantire che la tua infrastruttura di monitoraggio Amazon EKS rimanga affidabile e resiliente e che tu abbia una visibilità continua sui tuoi ambienti Kubernetes anche durante vari scenari di errore. I test e gli aggiornamenti regolari di queste configurazioni HA garantiscono che rimangano efficaci man mano che l'ambiente si evolve.

# Le migliori pratiche per il monitoraggio in Amazon EKS

## Approccio di implementazione strategico

Una strategia di monitoraggio Amazon EKS di successo inizia con un approccio di implementazione ben pianificato e graduale.

- Inizia identificando e monitorando i parametri critici che influiscono direttamente sulle operazioni aziendali e sull'affidabilità delle applicazioni. Questa base dovrebbe includere i parametri essenziali dell'infrastruttura, gli indicatori chiave delle prestazioni delle applicazioni e i parametri di sicurezza critici. Espandi gradualmente la copertura del monitoraggio in base alle esigenze operative e alle lezioni apprese e assicurati che ogni aggiunta fornisca un valore significativo.
- Implementa processi di implementazione automatizzati utilizzando strumenti di infrastruttura come codice (IaC) come Terraform o CloudFormation per garantire coerenza e ripetibilità.
- Testa e convalida i sistemi di monitoraggio per contribuire a mantenere l'affidabilità e la precisione.

- Perfeziona continuamente i parametri di monitoraggio in linea con le esigenze aziendali in evoluzione.

## Gestione efficace dei dati

Una corretta gestione dei dati è fondamentale per mantenere una soluzione di monitoraggio efficiente ed economica.

- Implementa politiche chiare di conservazione dei dati che bilanciano le esigenze di analisi storica con i costi di archiviazione.
- Configura le frequenze di campionamento appropriate per diversi tipi di metriche: frequenza più alta per le metriche critiche e frequenza più bassa per quelle meno critiche.
- Utilizza l'aggregazione delle metriche per ridurre il volume dei dati mantenendo al contempo informazioni significative, in particolare per l'analisi delle tendenze a lungo termine.
- Implementa procedure sistematiche di conservazione e archiviazione dei log per sistemi di registrazione centralizzati (come CloudWatch Logs) per gestire i costi di archiviazione e mantenere accessibile l'accesso ai dati importanti.

> **Note**
>
> La rotazione dei log a livello di contenitore viene gestita automaticamente dal kubelet in Amazon EKS versione 1.21 o successiva.

- Prendi in considerazione l'implementazione di un' hot-warm-coldarchitettura per l'archiviazione dei log per ottimizzare sia la velocità di accesso che l'efficienza dei costi.

## Configurazione e gestione degli avvisi

La configurazione degli avvisi richiede un'attenta valutazione per mantenere l'efficacia senza causare affaticamento degli avvisi.

- Definisci soglie chiare e attuabili in base agli obiettivi dei livelli di servizio (SLOs) e ai modelli prestazionali storici.
- Implementa un sistema di gravità degli avvisi a più livelli che distingua chiaramente tra questioni critiche che richiedono attenzione immediata e questioni meno urgenti.

- Assicurati che gli avvisi forniscano un contesto sufficiente e informazioni utilizzabili per facilitare una rapida risoluzione dei problemi.
- Stabilisci procedure di segnalazione chiare con titolarità e tempi di risposta definiti per diverse gravità degli avvisi.
- Rivedi e perfeziona regolarmente le configurazioni degli avvisi per mantenerne la pertinenza e l'efficacia.

## Ottimizzazione delle risorse

Il monitoraggio continuo dell'utilizzo delle risorse è essenziale per mantenere operazioni convenienti.

- Implementa il monitoraggio completo delle risorse su tutti i componenti del cluster, inclusi nodi, pod e volumi persistenti.
- Configura la scalabilità automatica in base ai modelli di utilizzo effettivi e ai requisiti prestazionali per garantire un utilizzo efficiente delle risorse mantenendo al contempo le prestazioni.
- Utilizza i tag di allocazione dei costi per tenere traccia del consumo di risorse da parte di diversi team, applicazioni o ambienti.
- Analizza regolarmente le metriche sull'efficienza delle risorse per identificare opportunità di ottimizzazione e implementare miglioramenti.
- Prendi in considerazione l'implementazione di strumenti di gestione dei costi per tracciare e ottimizzare la spesa per il cloud.

## Sicurezza

Le considerazioni sulla sicurezza dovrebbero essere parte integrante della tua strategia di monitoraggio.

- Implementa i principi di accesso con privilegio minimo per tutti i componenti di monitoraggio per garantire che utenti e servizi dispongano solo delle autorizzazioni di cui hanno bisogno.
- Abilita una registrazione di controllo completa per tenere traccia di tutti gli accessi e le modifiche ai sistemi di monitoraggio.
- Effettua regolari revisioni di sicurezza delle configurazioni di monitoraggio e dei modelli di accesso per identificare potenziali vulnerabilità.
- Implementa la crittografia per i dati di monitoraggio sensibili sia in transito che a riposo.

- Integra il monitoraggio della sicurezza con i sistemi SIEM (Security Information and Event Management) esistenti per una visibilità completa della sicurezza.

## Considerazioni sul monitoraggio avanzato in Amazon EKS

Ottimizzazione delle prestazioni:

- Ottimizza gli intervalli di raccolta delle metriche.
- Configura modelli di interrogazione efficienti.
- Implementa la preaggregazione delle metriche.
- Utilizza soluzioni di storage appropriate.

Conformità e governance:

- Mantieni gli audit trail.
- Implementa il monitoraggio della conformità.
- Fornisci rapporti di conformità regolari.
- Procedure di monitoraggio dei documenti.

Ripristino di emergenza:

- Esegui regolarmente il backup delle configurazioni di monitoraggio.
- Procedure di recupero dei documenti.
- Test dei processi di ripristino.

Miglioramento continuo:

- Monitora regolarmente le sessioni di revisione.
- Ottimizza i cicli di prestazioni.
- Aggiorna il monitoraggio in base agli incidenti.
- Incorpora il feedback degli utenti.

Queste best practice forniscono un framework per l'implementazione e il mantenimento di soluzioni di monitoraggio efficaci per gli ambienti Amazon EKS. Rivedi e aggiorna regolarmente queste

pratiche in modo che rimangano in linea con le esigenze organizzative e gli standard di settore. Il monitoraggio non è una configurazione una tantum, è un processo continuo che richiede un'attenzione e un perfezionamento regolari.

# Tracciamento in Amazon EKS

Il tracciamento è un componente fondamentale dell'osservabilità delle applicazioni in Amazon EKS. Il tracciamento fornisce una visibilità dettagliata dei flussi di richieste e delle interazioni di servizio raccogliendo, elaborando e visualizzando il percorso delle richieste mentre viaggiano attraverso vari microservizi distribuiti sui cluster EKS. Questa funzionalità ti aiuta a comprendere il comportamento del sistema, identificare i colli di bottiglia e risolvere i problemi in modo efficace nel tuo ambiente Amazon EKS. Un tracciamento efficace elimina la complessità del debug dei sistemi distribuiti fornendo visibilità sui flussi di richieste. end-to-end Consente di tenere traccia delle transazioni oltre i confini del servizio e identificare problemi o guasti di prestazioni all'interno dei carichi di lavoro di Amazon EKS.

L'implementazione complessiva del tracciamento in Amazon EKS consente di comprendere il comportamento del sistema, ottimizzare le prestazioni e mantenere l'affidabilità delle applicazioni containerizzate. In definitiva, le funzionalità di tracciamento migliorano la visibilità operativa e la manutenibilità del sistema negli ambienti Amazon EKS.

AWS X-Ray svolge un ruolo significativo nel tracciare i dati relativi alla tua applicazione. Il tracciamento implica il monitoraggio di vari aspetti delle interazioni del servizio, tra cui:

- I percorsi e le dipendenze delle richieste forniscono informazioni cruciali sul comportamento del sistema distribuito. Tracciano l'intero percorso delle richieste mentre attraversano diversi microservizi e componenti. La mappatura delle dipendenze dei servizi consente di comprendere i modelli di comunicazione e identificare i percorsi critici nell'architettura dell'applicazione. Per i dettagli sull'implementazione, vedere Utilizzo della mappa AWS X-Ray di tracciamento del servizio nella documentazione di X-Ray.
- Le latenze e i colli di bottiglia del servizio sono metriche essenziali per mantenere prestazioni ottimali del sistema. Misurando e analizzando i tempi di risposta tra i servizi, è possibile identificare efficacemente i problemi di prestazioni. Questi dati consentono di individuare servizi o operazioni specifici che causano ritardi nella catena di richieste e di consentire sforzi di ottimizzazione mirati. Per ulteriori informazioni sull'analisi della latenza, consulta Interagire con la console Analytics nella documentazione X-Ray.
- I modelli di propagazione degli errori aiutano a comprendere l'affidabilità del sistema e la tolleranza agli errori. Comprendendo in che modo gli errori si ripercuotono a cascata nel sistema e tracciando i percorsi di errore tra i servizi, è possibile progettare meglio le applicazioni. Questa visibilità consente di identificare la causa principale degli errori e il loro impatto sui servizi dipendenti,

il che porta a sistemi più resilienti. Per i dettagli sull'implementazione, vedere Traces nella documentazione di X-Ray.

- L'utilizzo delle risorse tra i servizi fornisce informazioni sull'efficienza del sistema e sull'ottimizzazione dei costi. È possibile monitorare i modelli di utilizzo della CPU, della memoria e della rete correlati ai dati di traccia per comprendere le richieste di risorse. Questi dati consentono di analizzare le tendenze del consumo di risorse per ottimizzare le prestazioni e i costi dei servizi in tutto il cluster EKS. Per la configurazione del monitoraggio, consulta Monitoraggio delle prestazioni del cluster e visualizzazione dei log nella documentazione di Amazon EKS.
- I flussi di transazioni degli utenti finali sono fondamentali per comprendere e migliorare l'esperienza dell'utente. Monitorando le interazioni complete degli utenti dai servizi di frontend a quelli di backend, è possibile garantire prestazioni ottimali delle applicazioni. È possibile misurare e ottimizzare i tempi di end-to-end risposta per i percorsi critici degli utenti, con un impatto diretto sulla soddisfazione del cliente. Per implementare il monitoraggio degli utenti finali, utilizzate l'AWS X-Ray SDK per il vostro linguaggio di programmazione.
- Le interazioni con i gateway API costituiscono la prima linea per quanto riguarda le prestazioni e la sicurezza dell'applicazione. È possibile monitorare i modelli di richiesta e le prestazioni nei punti di ingresso delle API per garantire un'erogazione ottimale del servizio. Questa visibilità consente di tenere traccia degli impatti di autenticazione, autorizzazione e limitazione della velocità sui flussi di richieste, per mantenere i requisiti di sicurezza e prestazioni. Scopri di più sul tracciamento delle API nella documentazione di Amazon API Gateway with X-Ray.

Un tracciamento efficace in Amazon EKS va oltre la semplice raccolta di intervalli e tracce. Richiede una strategia ben strutturata che bilanci le esigenze di osservabilità con le prestazioni del sistema. Questa strategia dovrebbe concentrarsi su:

- Implementazione di frequenze di campionamento appropriate: configura le regole di campionamento in base ai modelli di traffico e alle priorità aziendali per ottimizzare i costi mantenendo al contempo la visibilità delle transazioni critiche. Per ulteriori informazioni, vedere Configurazione delle regole di campionamento nella documentazione X-Ray.
- Definizione di percorsi e servizi critici da tracciare: identifica e dai priorità ai servizi essenziali e ai percorsi utente che richiedono una tracciatura dettagliata per garantire un monitoraggio ottimale delle prestazioni. Per ulteriori informazioni, consulta Inviare dati metrici e di tracciamento con ADOT Operator nella documentazione di Amazon EKS.
- Stabilire politiche di conservazione dei dati adeguate: imposta regole di gestione del ciclo di vita dei dati per bilanciare le esigenze di osservabilità con i costi di archiviazione e i requisiti di conformità.

Per visualizzare le politiche di CloudWatch conservazione, consulta Lavorare con gruppi di log e flussi di log nella documentazione dei log. CloudWatch

- Configurazione di strumenti di visualizzazione e analisi efficaci: distribuisci e configura strumenti di visualizzazione come la console AWS X-Ray Analytics o Amazon Managed Grafana per analizzare i dati di traccia in modo efficace. Per ulteriori informazioni, consulta Interagire con la console Analytics nella documentazione X-Ray.

In questa sezione:



# Strumenti di tracciamento per Amazon EKS

Amazon EKS supporta diverse opzioni AWS di terze parti per l'implementazione del tracciamento distribuito.

## Servizi AWS

- AWS X-Ray: piattaforma di tracciamento distribuito avanzata

  X-Ray è un sistema completamente gestito Servizio AWS che fornisce funzionalità di end-to-end tracciamento. Strumenta Servizi AWS e fornisce automaticamente mappe e analisi dettagliate dei servizi per le applicazioni eseguite su Amazon EKS. X-Ray è integrato con altri Servizi AWS, incluso Amazon CloudWatch, e offre la correlazione automatica delle tracce con le chiamate. Servizio AWS
- AWS Distro per OpenTelemetry: framework di osservabilità unificato

  Distro for OpenTelemetry è una distribuzione sicura, pronta per la produzione e AWS supportata per applicazioni native del cloud. OpenTelemetry Offre funzionalità di strumentazione indipendenti dal fornitore pur mantenendo l' Servizio AWS integrazione nativa, il che la rende ideale per gli ambienti cloud ibridi. Distro for OpenTelemetry supporta più backend di osservabilità e offre una perfetta integrazione con i servizi di monitoraggio. AWS

## Soluzioni open source

- OpenTelemetry: Framework di osservabilità open source

OpenTelemetry fornisce un framework di osservabilità standardizzato con librerie di strumentazione complete che supportano più linguaggi di programmazione. Le sue opzioni di backend flessibili e l'approccio indipendente dal fornitore lo rendono ideale per carichi di lavoro che richiedono coerenza tra diversi ambienti. L'ampio ecosistema del framework garantisce un'ampia compatibilità con varie soluzioni di monitoraggio.

- Jaeger: piattaforma di tracciamento distribuita open source

  Jaeger offre funzionalità di tracciamento complete con propagazione del contesto distribuita in tempo reale. Fornisce l'analisi delle cause principali e l'ottimizzazione delle prestazioni attraverso una visualizzazione dettagliata della dipendenza dal servizio. L'architettura di Jaeger è progettata per un'elevata scalabilità e supporta vari backend di storage, il che la rende adatta per implementazioni Amazon EKS su larga scala. Visualizza la configurazione di Jaeger for EKS
- Grafana Tempo: tracciamento distribuito

  Tempo è una soluzione Grafana Labs che fornisce l'archiviazione delle tracce su larga scala e una perfetta integrazione con le metriche di Prometheus. Il suo modello di conservazione delle tracce conveniente e l'integrazione nativa con Grafana lo rendono adatto alle organizzazioni che già utilizzano Grafana per la visualizzazione. L'architettura di Tempo è progettata specificamente per ambienti cloud nativi come Amazon EKS.

## Le migliori pratiche per il tracciamento in Amazon EKS

Questa sezione fornisce un elenco completo di best practice e tecniche per creare un sistema di tracciamento efficace che migliori l'osservabilità e la risoluzione dei problemi per le applicazioni basate su Kubernetes in Amazon EKS.

- Campionamento strategico: configura diverse frequenze di campionamento in base ai modelli di traffico dell'applicazione e all'importanza dei servizi che utilizzi. Implementa frequenze di campionamento più elevate per i percorsi critici, riducendo al contempo il campionamento per percorsi ad alto volume e meno critici per ottimizzare i costi. Per informazioni, consulta Configurazione delle regole di campionamento nella documentazione. AWS X-Ray
- Configurazione della strumentazione: utilizza strumenti di strumentazione automatici come X-Ray SDK o AWS Distro for Collector per OpenTelemetry ridurre al minimo lo sforzo di strumentazione manuale. Mantieni convenzioni di denominazione coerenti e una propagazione del contesto tra i servizi per una migliore correlazione delle tracce. Per ulteriori informazioni, consulta la documentazione di Distro for collector. OpenTelemetry

- Gestione dei dati: implementa periodi di conservazione e strategie di compressione appropriati per bilanciare i costi di archiviazione con le esigenze di osservabilità. Stabilisci controlli chiari sulla privacy dei dati e procedure di backup per proteggere i dati di traccia sensibili. Per ulteriori informazioni, consulta Change log data retention in CloudWatch Logs nella documentazione CloudWatch Logs.
- Ottimizzazione delle prestazioni: monitora e ottimizza il sovraccarico di tracciamento per ridurre al minimo l'impatto sulle prestazioni delle applicazioni. Utilizza un buffering efficiente e l'elaborazione asincrona per ridurre l'impatto sulla latenza. Per ulteriori informazioni, vedere Configurazione del AWS X-Ray demone nella documentazione X-Ray.
- Controlli di sicurezza: implementa controlli di accesso e misure di protezione dei dati adeguati utilizzando i ruoli e le politiche IAM. I controlli di sicurezza e le revisioni di conformità regolari aiutano a garantire che i dati di traccia rimangano sicuri. Per ulteriori informazioni, vedere Sicurezza AWS X-Ray nella documentazione X-Ray.
- Monitoraggio e avvisi: imposta un monitoraggio completo dello stato della raccolta di tracce e configura gli avvisi per i problemi di raccolta. Tieni traccia delle frequenze di campionamento e delle metriche delle prestazioni del sistema per garantire un funzionamento ottimale. Per ulteriori informazioni, consulta Container Insights nella CloudWatch documentazione.
- Alta disponibilità: implementa raccoglitori ridondanti nelle zone di disponibilità e configura meccanismi di failover adeguati. I test regolari della configurazione ad alta disponibilità garantiscono una raccolta affidabile delle tracce. Per ulteriori informazioni, consulta Using AWS Distro for OpenTelemetry as a collector nella documentazione di Amazon Managed Service for Prometheus.

Seguendo queste best practice, puoi creare un sistema di tracciamento solido, efficiente ed efficace per il tuo ambiente Amazon EKS. Ciò contribuirà a garantire un'osservabilità completa, una risoluzione dei problemi efficiente e prestazioni ottimali delle applicazioni basate su Kubernetes.

# Avvisi in Amazon EKS

Gli avvisi sono un componente fondamentale per la gestione e la manutenzione delle applicazioni eseguite su Amazon EKS. Funge da sistema di allarme rapido che notifica a operatori e sviluppatori potenziali problemi, anomalie o peggioramenti delle prestazioni prima che si trasformino in problemi gravi che potrebbero influire sulla disponibilità del servizio o sull'esperienza dell'utente. L'invio di avvisi implica il monitoraggio di vari aspetti del cluster Kubernetes, tra cui:

- Stato dell'infrastruttura
- Prestazioni delle applicazioni
- Parametri dei container
- Metriche aziendali personalizzate

L'efficacia degli avvisi in Amazon EKS va oltre la semplice configurazione delle notifiche. Richiede una well-thought-out strategia che bilanci la necessità di informazioni tempestive con il potenziale rischio di sovraccarico. Questa strategia dovrebbe:

- Definire soglie e condizioni significative.
- Assegna priorità agli avvisi in base alla gravità e all'impatto.
- Implementa procedure di routing ed escalation adeguate.
- Integrazione con gli strumenti di gestione e comunicazione degli incidenti.

In questa sezione:



## Strumenti di avviso per Amazon EKS

Amazon EKS supporta diverse opzioni AWS di terze parti per l'implementazione degli avvisi. Quando scegli uno strumento per gli avvisi di Amazon EKS, prendi in considerazione fattori quali capacità di integrazione, scalabilità, facilità d'uso, costi e funzionalità specifiche in linea con i tuoi requisiti di monitoraggio e avviso. Molte organizzazioni utilizzano una combinazione di questi strumenti per creare una soluzione completa di monitoraggio e avviso per i propri ambienti Amazon EKS.

- Amazon CloudWatch: Servizio AWS per il monitoraggio e l'osservabilità

  CloudWatch fornisce metriche, registri e allarmi per i cluster EKS e si integra bene con altri. Servizi AWS
- Prometheus: strumento di monitoraggio e avviso open source per Kubernetes

  Prometheus fornisce un potente linguaggio di interrogazione (PromQL) per definire le condizioni di avviso.
- Alertmanager: complemento di Prometheus per la gestione degli avvisi

  Alertmanager fornisce la deduplicazione, il raggruppamento e il routing degli avvisi. Supporta vari canali di notifica, tra cui e-mail, Slack e. PagerDuty
- Grafana: piattaforma open source per il monitoraggio e l'osservabilità

  Grafana offre funzionalità di visualizzazione e avviso. Può integrarsi con varie fonti di dati, tra cui Prometheus e. CloudWatch
- Elastic Stack (ELK Stack): combinazione di Elasticsearch, Logstash e Kibana

  Questo strumento è utile per l'aggregazione, l'analisi e l'invio di avvisi dei log. Può essere esteso con le funzionalità di osservabilità di Elastic.
- Soluzioni di terze parti

  Sul mercato sono disponibili molti strumenti, tra cui Datadog, New Relic, Sysdig, Dynatrace, Zabbix, Nagios, Splunk, IBM Instana e. AppDynamics

## Le migliori pratiche per la generazione di avvisi in Amazon EKS

Questa sezione descrive le migliori pratiche per creare un solido sistema di avvisi che migliori l'affidabilità e le prestazioni delle applicazioni basate su Kubernetes in Amazon EKS.

Definisci soglie di avviso chiare:

- Imposta soglie significative basate su dati storici e requisiti aziendali.
- Utilizza soglie dinamiche laddove appropriato per tenere conto dei diversi carichi di lavoro.

Implementa la prioritizzazione degli avvisi:

- Categorizza gli avvisi in base alla gravità (ad esempio, critico, alto, medio, basso).

- Allinea le priorità degli avvisi all'impatto aziendale.

Evita l'affaticamento da allarme:

- Riduci il rumore eliminando gli avvisi ridondanti o di basso valore.
- Correla gli avvisi ai problemi relativi al gruppo.

Usa avvisi in più fasi:

- Implementa soglie di avviso prima che vengano raggiunti i livelli critici.
- Utilizza canali di notifica diversi per livelli di gravità degli avvisi diversi.

Implementa il routing corretto degli avvisi:

- Assicurati che gli avvisi vengano inviati ai team o alle persone giuste.
- Utilizza gli orari e le rotazioni di chiamata per una copertura completa e giornaliera.

Sfrutta le metriche native di Kubernetes:

- Monitora i componenti principali di Kubernetes (nodi, pod, servizi).
- Usa kube-state-metrics (KSM) per metriche aggiuntive degli oggetti Kubernetes.

Monitora sia l'infrastruttura che le applicazioni:

- Imposta avvisi per lo stato del cluster, lo stato dei nodi e l'utilizzo delle risorse.
- Implementa avvisi specifici dell'applicazione, ad esempio tassi di errore e latenza.

Usa Prometheus e Alertmanager:

- Usa Prometheus per la raccolta delle metriche e PromQL per definire le condizioni di avviso.
- Usa Alertmanager per il routing e la deduplicazione degli avvisi.

Integrazione con Amazon CloudWatch:

- Usa CloudWatchContainer Insights per i parametri specifici di Amazon EKS.

- Imposta CloudWatchallarmi per i parametri critici delle risorse. AWS

Implementa avvisi contestuali:

- Includi informazioni pertinenti nei messaggi di avviso, come il nome del cluster, lo spazio dei nomi e i dettagli del pod.
- Fornisci collegamenti a dashboard o runbook pertinenti negli avvisi.

Usa il rilevamento delle anomalie:

- Implementa il rilevamento delle anomalie basato sull'apprendimento automatico per modelli complessi.
- Utilizza servizi come il rilevamento delle CloudWatch anomalie o strumenti di terze parti.

Implementa la soppressione e il silenziamento degli avvisi:

- Consenti la soppressione temporanea dei problemi noti.
- Implementa finestre di manutenzione per ridurre il rumore durante i periodi di inattività pianificati.

Monitora le prestazioni degli avvisi:

- Tieni traccia di metriche come la frequenza degli avvisi, il tempo di risoluzione e le percentuali di falsi positivi.
- Rivedi e perfeziona regolarmente le regole di avviso in base a queste metriche.

Implementa procedure di escalation:

- Definisci percorsi di escalation chiari per gli avvisi irrisolti.
- Utilizza strumenti come Opsgenie per le PagerDuty escalation automatizzate.

Testa regolarmente i sistemi di allarme:

- Eseguite test periodici della vostra pipeline di avvisi.
- Includi i test degli avvisi nelle esercitazioni di disaster recovery.

Utilizza i modelli per la coerenza degli avvisi:

- Crea modelli di avviso standardizzati per scenari comuni.
- Garantisci formattazione e informazioni coerenti in tutti gli avvisi.

Implementa la limitazione della velocità:

- Previeni le tempeste di avvisi implementando la limitazione della velocità sugli avvisi attivati di frequente.

Usa metriche personalizzate:

- Implementa metriche personalizzate per il monitoraggio specifico dell'applicazione.
- Utilizza l'API Kubernetes Custom Metrics per il ridimensionamento automatico basato su queste metriche.

Implementa l'integrazione della registrazione:

- Correla gli avvisi con i registri pertinenti per una risoluzione più rapida dei problemi.
- Usa strumenti come Grafana Loki o ELK Stack insieme al tuo sistema di avviso.

Prendi in considerazione gli avvisi sui costi:

- Imposta avvisi in caso di picchi imprevisti nell'utilizzo delle risorse o nei costi.
- Utilizza strumenti Budget AWSdi gestione dei costi di terze parti.

Usa la tracciabilità distribuita:

- Integra strumenti di tracciamento distribuiti come Jaeger o. AWS X-Ray
- Imposta avvisi per modelli di traccia o latenze anomali.

Runbook per gli avvisi relativi ai documenti:

- Crea runbook chiari e utilizzabili per ogni tipo di avviso.
- Includi passaggi per la risoluzione dei problemi e procedure di escalation nei runbook.

Seguendo queste best practice, puoi creare un sistema di avvisi robusto, efficiente ed efficace per il tuo ambiente Amazon EKS. Ciò contribuirà a garantire un'elevata disponibilità, una rapida risoluzione dei problemi e prestazioni ottimali delle applicazioni basate su Kubernetes.

# Fasi successive

Questa guida ha fornito un framework completo per implementare una solida osservabilità negli ambienti Amazon EKS, concentrandosi sulla raccolta di metriche, l'infrastruttura di registrazione, la tracciabilità distribuita e l'ottimizzazione dei costi. Comprendendo e applicando questi componenti principali, puoi creare un ambiente container altamente osservabile, gestibile ed economico che fornisce informazioni approfondite sul comportamento delle applicazioni e dell'infrastruttura. L'integrazione di Servizi AWS Amazon CloudWatch Container Insights e AWS X-Ray, combinata con soluzioni open source come Prometheus e, crea una solida base per il monitoraggio OpenTelemetry e la risoluzione dei problemi delle applicazioni containerizzate.

Il successo dell'implementazione si basa su un approccio graduale, che inizia con la raccolta delle metriche di base e si estende gradualmente a funzionalità complete di registrazione e tracciamento distribuito. Ti consigliamo di iniziare valutando le tue attuali capacità di monitoraggio, identificando le lacune e selezionando le combinazioni di strumenti appropriate in linea con i requisiti operativi e l'esperienza del team. Questo approccio metodico garantisce che ogni componente dello stack di osservabilità sia correttamente implementato e integrato, mentre i team sviluppano le competenze e i processi necessari per utilizzare efficacemente questi strumenti.

La sostenibilità a lungo termine dell'osservabilità di Amazon EKS dipende dall'ottimizzazione regolare di costi, risorse e processi. È necessario rivedere e modificare continuamente la propria infrastruttura di osservabilità, comprese le politiche di conservazione dei dati, le frequenze di campionamento e l'allocazione delle risorse, per mantenere il giusto equilibrio tra monitoraggio completo ed efficienza operativa. Questo approccio iterativo al miglioramento, combinato con la formazione continua del team e gli aggiornamenti della documentazione, consente all'organizzazione di mantenere un'osservabilità efficace, supportando al contempo la crescita aziendale e l'adattamento alle architetture applicative in evoluzione.

# Risorse

## AWS documentazione

- Guida alle best practice di Amazon EKS
- Amazon CloudWatch Container Insights
- Amazon Managed Service per Prometheus
- Amazon Managed Grafana
- AWS Distro per OpenTelemetry e AWS X-Ray
- OpenSearch Servizio Amazon

## AWS post sul blog

- Amazon EKS migliora l'osservabilità del piano di controllo Kubernetes
- Automatizzazione della raccolta di metriche su Amazon EKS con Amazon Managed Service per gli scraper gestiti Prometheus
- Automatizza il monitoraggio per il tuo cluster Amazon EKS utilizzando CloudWatch Container Insights
- Migliorare l'osservabilità con una soluzione di monitoraggio gestita per Amazon EKS

## Altre risorse

- Documentazione di OpenTelemetry
- Documentazione Prometheus
- Documentazione Fluent Bit
- Monitoraggio, registrazione e debug nella documentazione di Kubernetes

# 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 |
| --- | --- | --- |
| Aggiornamenti | Abbiamo aggiornato il capitolo Logging in Amazon EKS. | 17 marzo 2026 |
| Pubblicazione iniziale | — | 10 aprile 2025 |

# AWS Glossario delle linee guida prescrittive

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

## Numeri

7 R

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

- 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 in genere includono addetti alle 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. Per ulteriori informazioni, consulta la guida Quantificazione dell'incertezza nei sistemi di deep learning.

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.