Guida alla registrazione e al monitoraggio per i proprietari delle applicazioni

AWS Guida prescrittiva

AWS Guida prescrittiva: Guida alla registrazione e al monitoraggio per i proprietari delle applicazioni

Table of Contents

Guida alla registrazione e al monitoraggio per i proprietari delle applicazioni

John Buckley, Amazon Web Services (AWS)

Gennaio 2023 (cronologia del documento)

Un carico di lavoro è una raccolta di risorse e codice che fornisce valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo back-end. Un carico di lavoro può essere costituito da un sottoinsieme di risorse in un unico Account AWS o potrebbe estendersi su più Account AWS. Nel cloud, un'applicazione è un tipo di carico di lavoro. Potrebbe essere distribuita esclusivamente nell'ambiente cloud oppure potrebbe essere supportata anche da hardware on-premise locale. Molte pubblicazioni si concentrano sulla registrazione e sul monitoraggio dell'infrastruttura cloud e sono destinate ai team di sicurezza. Questa guida è destinata ai proprietari di applicazioni e si concentra su approcci efficaci ed efficienti per la registrazione e il monitoraggio delle applicazioni nel Cloud AWS.

Questa guida consente di impostare la registrazione e il monitoraggio a un livello appropriato in modo da poter identificare e rispondere rapidamente alle anomalie. Inoltre, consente di verificare che i log delle applicazioni supportino l'analisi dettagliata e la risoluzione di eventuali problemi.

Sebbene questa guida sia stata scritta pensando alle implementazioni di Cloud AWS, è possibile applicare questi principi alle applicazioni eseguite on-premise o su un'altra infrastruttura di provider di cloud.

Obiettivi aziendali specifici

Dopo aver letto questa guida dovresti essere in grado di individuare:

- I tipi di eventi che vengono comunemente registrati per le applicazioni
- Gli attributi degli eventi (ad esempio who, what e when) da considerare per la registrazione
- I tipi di dati da escludere dai log, ad esempio i dati che potrebbero compromettere il livello di sicurezza o le informazioni di identificazione personale
- Come impostare la registrazione e il monitoraggio a un livello appropriato per l'applicazione
- Chi dovrebbe essere in grado di gestire e accedere ai log delle applicazioni

- I Servizi AWS e le funzionalità che è possibile configurare per monitorare e registrare le applicazioni nel Cloud AWS
- Come utilizzare i dati di log dell'applicazione e Servizi AWS e funzionalità per la valutazione e la diagnosi dei problemi

Informazioni sulla registrazione e sul monitoraggio delle applicazioni

La registrazione, il monitoraggio, gli avvisi e i report sono diversi processi di sicurezza che interagiscono per fornire visibilità sullo stato e sulle prestazioni dell'applicazione. È fondamentale creare e mantenere un record dettagliato delle azioni e degli eventi relativi all'applicazione in modo da poter monitorare, avvisare e generare report basati sull'attività registrata.

La registrazione delle applicazioni è il processo di raccolta degli eventi generati dall'applicazione e di registrazione degli eventi in uno o più file di log. Questa cronologia degli eventi può aiutare a eseguire analisi di sicurezza e prestazioni, tenere traccia delle modifiche alle risorse e risolvere i problemi delle applicazioni.

Il monitoraggio delle applicazioni è il processo di valutazione delle prestazioni e dello stato complessivi dell'applicazione. Dovresti essere in grado di monitorare costantemente il frontend e il backend dell'applicazione. Poiché le applicazioni ospitate sul cloud sono altamente distribuite, gli strumenti di registrazione e monitoraggio possono aiutarti a risolvere rapidamente i problemi di prestazioni o a identificare e porre rimedio alle minacce alla sicurezza in tempo reale. I dati di log sono un input fondamentale per il monitoraggio.

L'osservabilità è simile al monitoraggio, ma introduce modi per misurare il comportamento delle applicazioni utilizzando parametri diversi e consente correlazioni complesse. Un esempio è la misurazione della percentuale di successo HTTP in un determinato giorno, per un insieme di utenti in una regione geografica specifica. Per ulteriori informazioni, consulta la pagina Monitoraggio e osservabilità (marketing AWS).

In definitiva, l'obiettivo dei proprietari delle applicazioni è quello di mantenere applicazioni sicure e integre e un'esperienza utente positiva con tali applicazioni. Implementando la registrazione e il monitoraggio, gli sviluppatori e i team operativi possono pianificare e risolvere più rapidamente i problemi delle applicazioni.

Il livello di registrazione e monitoraggio richiesto varia a seconda dell'applicazione. I fattori che possono influire sui livelli di monitoraggio e registrazione includono le politiche e le procedure organizzative, il livello di rischio per la sicurezza rappresentato dall'applicazione, la criticità dell'applicazione per le operazioni aziendali e la sensibilità dei dati gestiti dall'applicazione. In generale, le applicazioni pubbliche o rivolte ai clienti richiedono un livello di monitoraggio e registrazione più elevato rispetto alle applicazioni utilizzate internamente all'organizzazione. Questa

guida include informazioni e consigli generali e consigliamo di personalizzare l'approccio in base ai requisiti dell'applicazione.

> **Note**
>
> Gli standard o le procedure dell'organizzazione potrebbero imporre attributi specifici di registrazione e monitoraggio. Un esempio è il trasferimento delle autorizzazioni degli utenti a un sistema di revisione delle autorizzazioni aziendali. Assicurati che il tuo piano di registrazione e monitoraggio soddisfi i requisiti della tua organizzazione.

Registrazione delle applicazioni nel Cloud AWS

Per la registrazione delle applicazioni nel Cloud AWS, esamina i tipi più comuni di eventi, gli attributi degli eventi e le best practice.

Questa sezione contiene gli argomenti seguenti:

Event types (Tipi di evento)

Una delle considerazioni più importanti quando si stabilisce una strategia di registrazione delle applicazioni è decidere quali eventi e azioni registrare. Sebbene i requisiti dell'organizzazione e dell'applicazione possano influire su questa decisione, si consiglia di registrare sempre quanto segue, se applicabile alla propria applicazione:

- Errori di convalida dell'input: gli esempi includono violazioni del protocollo, codifiche inaccettabili e nomi e valori di parametri non validi.
- Errori di convalida dell'output: gli esempi includono le mancate corrispondenze dei set di record del database e la codifica dei dati non valida.
- Successi e fallimenti dell'autenticazione dell'identità: registra le attività di autenticazione, ma non registra i nomi utente e le password. Poiché gli utenti possono digitare accidentalmente le proprie password in un campo del nome utente, si consiglia di non registrare i nomi utente. Le credenziali potrebbero essere rivelate involontariamente e comportare un accesso autorizzato. Implementare controlli di sicurezza per tutti i log che contengono dati di autenticazione.
- Errori di autorizzazione (controllo dell'accesso): per i sistemi di autorizzazione correlati, registra i tentativi di accesso non riusciti. È possibile monitorare questi dati di log per individuare modelli che potrebbero indicare un attacco o problemi con il sistema di autorizzazione dell'applicazione.
- Errori di gestione delle sessioni: gli esempi includono la modifica dei cookie o dei token di sessione. Le applicazioni utilizzano spesso cookie o token per gestire gli stati degli utenti. Gli utenti malintenzionati possono tentare di modificare i valori dei cookie per ottenere un accesso non autorizzato. La registrazione dei token di sessione alterati consente di rilevare questo comportamento.

- Errori dell'applicazione ed eventi di sistema: gli esempi includono errori di sintassi e di runtime, problemi di connettività, problemi di prestazioni, messaggi di errore provenienti da servizi di terze parti, errori del file system, rilevamento di virus per il caricamento di file e modifiche alla configurazione.
- Stato dell'applicazione: avvio o arresto dell'applicazione e delle relative risorse.
- Stato di registrazione: avvio, arresto o sospensione della registrazione.
- Utilizzo di funzionalità ad alto rischio: gli esempi includono modifiche alla connessione di rete, aggiunta o eliminazione di utenti, modifica dei privilegi, assegnazione di utenti a token, aggiunta o eliminazione di token, utilizzo dei privilegi amministrativi di sistema, accesso da parte degli amministratori delle applicazioni, tutte le azioni eseguite dagli utenti con privilegi amministrativi, accesso ai dati dei titolari di carte di pagamento, utilizzo di chiavi di crittografia dei dati, modifica delle chiavi di crittografia, creazione ed eliminazione di oggetti a livello di sistema, invio di contenuti generati dall'utente (in particolare caricamenti di file) e importazione ed esportazione di dati (compresi i report).
- Opt-in legali e di altro tipo: gli esempi includono le autorizzazioni per le funzionalità di telefonia mobile, i termini di utilizzo, i termini e le condizioni, il consenso all'utilizzo dei dati personali e le autorizzazioni per ricevere comunicazioni di marketing.

Oltre agli attributi consigliati, per la tua applicazione, valuta quali attributi aggiuntivi potrebbero fornire dati utili per il monitoraggio, gli avvisi e i report. Esempi includono:

- Errori di sequenziamento
- Attributi che consentono di valutare il comportamento dell'utente che viola la politica di utilizzo accettabile dell'organizzazione
- Modifiche dei dati
- Attributi necessari per conformarsi a standard o regolamenti, come la prevenzione dei reati finanziari, la limitazione del trading azionario o la raccolta di informazioni sanitarie o di altre informazioni personali.
- Attributi che aiutano a identificare comportamenti sospetti o imprevisti, come i tentativi di eseguire azioni non autorizzate
- Modifiche di configurazione
- Modifiche al file di codice o alla memoria dell'applicazione

Attributi di eventi

Ogni voce di log deve includere informazioni sufficientemente dettagliate per il monitoraggio e l'analisi. È possibile registrare i dati completi del contenuto, ma è più efficace registrare le proprietà di estrazione o di riepilogo. I log delle applicazioni devono registrare le proprietà when, where, who, what e which di ciascun evento. Queste proprietà saranno diverse a seconda dell'architettura, della classe di applicazione e del sistema o dispositivo host.

Per la registrazione di data e ora, utilizza il Coordinated Universal Time (UTC) e i formati di data e ora riconosciuti a livello internazionale in ISO 8601 (sito Web ISO).

> **Note**
>
> Prendi in considerazione l'utilizzo di un servizio di sincronizzazione dell'ora di rete per garantire data e ora accurate. Amazon fornisce il servizio di sincronizzazione oraria di Amazon che viene utilizzato da molti Servizi AWS, incluso Amazon Elastic Compute Cloud (Amazon EC2). Il servizio di sincronizzazione oraria di Amazon utilizza un parco istanze di orologi atomici di riferimento con connessione satellitare in ciascuna Regione AWS per garantire misurazioni accurate dell'orario standard globale UTC tramite Network Time Protocol (NTP). Per ulteriori informazioni, consulta Tenere il tempo con il servizio di sincronizzazione oraria di Amazon (post sul blog di AWS).

I seguenti attributi di evento sono generalmente inclusi nei log.

Categoria di attributi	Attributi di evento	Descrizione
Quando	Data e ora di registrazione	Registra la data e l'ora in cui l'evento è stato aggiunto al log.
	Data e ora dell'evento	Registra la data e l'ora in cui si è verificato l'evento. Questo record potrebbe essere diverso dal record di registrazione, ad esempio quando la registrazione viene ritardata

		perché l'applicazione client è ospitata su un dispositivo remoto che è online periodica mente o in modo intermittente.
	Identificatore di eventi	Registra un nome utente, un numero di account o un altro attributo univoco che assicuri che l'evento possa sempre essere identificato.
Where	Identificatore dell'applicazione	Registra il nome e la versione dell'applicazione.
	Indirizzo dell'applicazione	Registra il cluster o il nome host, l'indirizzo IPv4 o IPv6 del server, il numero di porta, l'identità della workstation e l'identificatore del dispositivo locale.
	Servizio	Registra il nome e il protocollo del servizio.
	GeoLocation	Registra le posizioni geografic he dell'utente.
	Finestra, modulo o pagina	Registra l'URL del punto di ingresso, il metodo HTTP per un'applicazione Web o il nome della finestra di dialogo in cui è stata eseguita l'azione.
	Posizione del codice	Registra il nome dello script o del modulo.

Who (utente umano o macchina)	Indirizzo di origine	Registra l'identificatore del dispositivo, l'indirizzo IP, l'ID della torre cellulare o a radiofrequenza (RF) o il numero di cellulare dell'utente.
	Identità utente	Se l'utente è autenticato o altrimenti conosciuto, registra il valore della chiave primaria, il nome utente o il numero di licenza della tabella del database utente.
	Classificazione dei tipi di utente	Registra il tipo di utente, ad esempio pubblico, autenticato, CMS, motore di ricerca, tester di penetrazione autorizza to o sistema di monitorag gio dell'uptime. Per ulteriori informazioni sui controlli di uptime, consulta Avvertenze ed esclusioni in questa guida.
	Richiedi intestazioni HTTP o agente utente HTTP	(Solo applicazioni Web) Registra le informazioni sull'intestazione della richiesta HTTP, inclusa la stringa dell'agente utente HTTP, poiché questi valori influiscono sulle informazioni che il client invia al server.
What	Tipo di evento	Registra se l'evento è informati vo, un avviso o un errore.

Gravità dell'evento	Classifica la gravità dell'evento, ad esempio alta, media e bassa.
Flag dell'evento di sicurezza	Se il log contiene dati non correlati agli eventi di sicurezza, crea un flag per gli eventi relativi alla sicurezza per identificarli.
Descrizione dell'evento	(Facoltativo) Include una breve descrizione dell'evento.
Azione o intento	Registra lo scopo originale previsto della richiesta, ad esempio l'accesso, l'aggiornamento dell'ID di sessione, la disconnessione o l'aggiornamento di un profilo.
Risposta dell'utente o dell'applicazione	Registra la risposta dell'utente o dell'applicazione all'evento, ad esempio un codice di stato, messaggi di testo personalizzati, l'interruzione della sessione o gli avvisi dell'amministratore.
Stato dei risultati	Registra se l'azione è stata eseguita correttamente, ad esempio azione riuscita, azione non riuscita o azione rinviata.

	Motivo del risultato	Registra il motivo per cui si è verificato lo stato. Ad esempio, una richiesta di accesso potrebbe non riuscire perché l'utente non è autenticato nel database.
	Dettagli estesi	Registra tutte le informazioni aggiuntive associate all'event o, ad esempio una traccia dello stack, i messaggi di errore di sistema, le informazi oni di debug e il corpo della richiesta HTTP.
	Codice di stato della risposta HTTP	(Solo applicazioni Web) Registra il codice di stato della risposta HTTP restituito all'utente, ad esempio `200` o `301`. Per ulteriori informazioni sul tagging, consulta Livelli di registrazione in questa guida.
Which	Risorse interessate	Registra quali risorse sono state utilizzate.
	Oggetto	Registra i componenti o altri oggetti interessati, ad esempio un account utente, una risorsa dati, un file, un URL o un ID di sessione.
	Nome della risorsa	Registra i nomi delle risorse interessate.

	Tag delle risorse	Registra i tag assegnati alla risorsa interessata. Per ulteriori informazioni sui tag, consulta Assegnazione di tag alle risorse AWS (Guida generale di riferimento di AWS).
Altro	Affidabilità analitica	Registra l'affidabilità del servizio di registrazione nel rilevamento degli eventi, ad esempio assegnando un punteggio basso, medio o alto o un valore numerico.
	Classificazioni interne	Registra tutte le classific azioni interne per verificarne l'aderenza agli standard o alla conformità.
	Classificazioni esterne	Registra eventuali classific azioni esterne per verificar ne l'aderenza agli standard o alla conformità, come il NIST Security Content Automation Protocol (SCAP).

Registrazione di best practice

Livelli di registrazione

Non registrare una quantità eccessiva di dati. I log devono acquisire dati utili e utilizzabili. Una registrazione eccessiva può influire negativamente sulle prestazioni e può anche aumentare i costi di archiviazione ed elaborazione della registrazione. Una registrazione eccessiva può inoltre far sì che problemi ed eventi di sicurezza non vengano rilevati.

La registrazione dei codici di stato della risposta HTTP può generare una quantità significativa di dati di log, in particolare codici di stato a 200 livelli (successo) e a 300 livelli (reindirizzamento). Si consiglia di prendere in considerazione la registrazione solo dei codici di stato a 400 livelli (errori lato client) e a 500 livelli (errori lato server).

I framework di registrazione delle applicazioni offrono diversi livelli di registrazione, ad esempio informazioni, debug o errore. Per gli ambienti di sviluppo, è possibile utilizzare la registrazione dettagliata, includendo, ad esempio, informazioni e debug, per aiutare gli sviluppatori. Tuttavia, consigliamo di disabilitare i livelli informazioni e debug per gli ambienti di produzione perché possono generare dati di registrazione eccessivi.

Avvertenze ed esclusioni

- Assicurati che i dati che stai registrando siano legalmente consentiti, in particolare nelle giurisdizioni in cui opera la tua organizzazione.
- Non escludere alcun evento riguardante utenti noti (ad esempio, altri sistemi interni), terze parti affidabili, robot dei motori di ricerca, sistemi di monitoraggio dell'uptime o dei processi e altri sistemi di monitoraggio remoto. Tuttavia, puoi includere un flag di classificazione per ognuno di questi nei dati registrati. I file di log generati dall'applicazione potrebbero essere utilizzati da soggetti, come soluzioni di monitoraggio dei log di terze parti o fornitori di servizi esterni, che non sono autorizzati a visualizzare i dati sensibili elaborati dall'applicazione.
- I seguenti attributi non devono essere registrati direttamente nei log. Rimuovi, maschera, sanitizza, codifica o cripta i seguenti dati:
  - Codice sorgente dell'applicazione
  - Valori di identificazione della sessione (valuta la possibilità di sostituirli con un valore con hash se devi tenere traccia degli eventi specifici della sessione)
  - Token di accesso
  - Dati personali sensibili e alcune forme di informazioni di identificazione personale (PII), come informazioni sanitarie o identificatori emessi dal governo
  - Password di autenticazione
  - Stringhe di connessione al database
  - Chiavi di crittografia e altri segreti primari
  - Dati del titolare del conto bancario o della carta di pagamento
  - È consentito archiviare dati con una classificazione di sicurezza più elevata rispetto al sistema di registrazione

- Informazioni commerciali sensibili
- Informazioni che è illegale raccogliere nelle giurisdizioni pertinenti
- Informazioni che un utente ha scelto di non accettare o che non ha esplicitamente acconsentito a raccogliere
- Informazioni per le quali il consenso alla raccolta è scaduto

Tipi di dati speciali

A volte, i seguenti dati possono essere registrati anche nei log. Sebbene ciò possa essere utile per scopi investigativi e di risoluzione dei problemi, può rivelare informazioni sensibili sul sistema. Potrebbe essere necessario rendere anonimi, eseguire l'hash o crittografare questi tipi di dati prima che l'evento venga registrato:

- Percorsi di file
- Nomi e indirizzi delle reti interne
- Dati personali non sensibili, come nomi personali, numeri di telefono e indirizzi e-mail

Utilizza l'anonimizzazione dei dati se la vera identità dell'individuo non è richiesta nel log o se il rischio è considerato eccessivo.

Gestione degli accessi e delle modifiche

- Gli utenti non amministrativi non dovrebbero essere in grado di disabilitare la registrazione degli eventi, in particolare quelli necessari per soddisfare i requisiti di conformità.
- Solo gli utenti amministrativi dovrebbero essere in grado di sospendere o interrompere i servizi di registrazione o modificare le configurazioni.
- Se il servizio di registrazione dispone di una funzionalità di convalida dell'integrità dei file di log, abilitala. Ciò consente di rilevare modifiche, eliminazioni o falsificazioni dei file di log. Per ulteriori informazioni su questa funzionalità nei Servizi AWS vedi Utilizzo di CloudTrail in questa guida.
- La registrazione delle modifiche deve essere intrinseca all'applicazione, ad esempio deve essere effettuata automaticamente dall'applicazione sulla base di un algoritmo approvato, oppure seguire processi di gestione delle modifiche approvati, ad esempio quando si cambiano i dati di configurazione o si modifica il codice sorgente.

Servizi AWS per la registrazione e il monitoraggio

Questa guida si concentra sulle applicazioni di registrazione e monitoraggio distribuite nel Cloud AWS. Puoi usare i Servizi AWS per implementare il tuo piano di registrazione e monitoraggio oppure puoi usarli per incrementare le tue soluzioni attuali. Ad esempio, se stai risolvendo un problema con la tua applicazione, puoi:

- Eseguire il triage dei log delle applicazioni con la funzionalità Log di flusso VPC in Amazon Virtual Private Cloud (Amazon VPC) e visualizzare il traffico di rete corrispondente al problema.
- Utilizzare AWS CloudTrail per visualizzare le chiamate API che corrispondono agli orari degli eventi problematici.
- Esaminare i log in File di log Amazon CloudWatch per verificare la presenza di picchi di CPU corrispondenti agli orari degli eventi problematici.

Puoi distribuire i seguenti Servizi AWS e le funzionalità per la registrazione e il monitoraggio dell'applicazione:

- AWS CloudTrail ti consente di controllare la governance, la conformità e il rischio operativo del tuo Account AWS registrando le azioni intraprese da un utente, un ruolo o un Servizio AWS. Per ulteriori informazioni sull'utilizzo di questo servizio per la registrazione o il monitoraggio di eventi per l'applicazione, consulta CloudTrail in questa guida.
- Amazon CloudWatch ti aiuta ad analizzare i log e, in tempo reale, a monitorare le metriche delle risorse AWS e delle applicazioni ospitate. Puoi anche utilizzare la funzionalità ServiceLens per controllare lo stato della tua applicazione o utilizzare la funzionalità Synthetics per creare canary che monitorano i tuoi endpoint e le tue API. Per ulteriori informazioni sull'utilizzo di questo servizio per monitorare la tua applicazione, consulta CloudWatch in questa guida.
- File di log Amazon CloudWatch ti aiuta a centralizzare i log di tutti i tuoi sistemi, applicazioni e Servizi AWS in modo da poterli monitorare e archiviare in modo sicuro. Per ulteriori informazioni sull'utilizzo di questo servizio per la registrazione di eventi per l'applicazione, consulta CloudWatch Logs in questa guida.
- La funzionalità Log di flusso VPC di Amazon Virtual Private Cloud (Amazon VPC) consente di acquisire informazioni sul traffico IP da e verso le interfacce di rete nel VPC. Per ulteriori informazioni sull'utilizzo di questo servizio per la registrazione di eventi per l'applicazione, consulta Log di flusso VPC in questa guida.

- AWS X-Ray raccoglie i dati sulle richieste gestite dall'applicazione e consente di visualizzare, filtrare e analizzare i dati per identificare i problemi e le opportunità di ottimizzazione. Per ulteriori informazioni sull'utilizzo di questo servizio per monitorare la tua applicazione, consulta X-Ray in questa guida.

Registrazione e monitoraggio di applicazioni tramite AWS CloudTrail

AWS CloudTrail è un Servizio AWS che aiuta a gestire l'auditing operativo e dei rischi, la governance e la conformità del tuo Account AWS. Le operazioni eseguite da un utente, un ruolo o un Servizio AWS vengono registrate come eventi in CloudTrail. Gli eventi possono includere le operazioni eseguite nella AWS Management Console, AWS Command Line Interface (AWS CLI) e nelle SDK e API AWS.

Utilizzo di CloudTrail

CloudTrail è abilitato sul tuo Account AWS al momento della sua creazione. Quando si verifica un'attività nel tuo Account AWS, tale attività viene registrata in un evento CloudTrail. Puoi visualizzare facilmente gli eventi recenti nella console CloudTrail accedendo a Cronologia di eventi.

Per un record continuo di attività ed eventi nel tuo Account AWS, puoi creare un trail. È possibile creare trail per una singola Regione AWS o per tutte le regioni. I trail registrano i file di log in ogni regione e CloudTrail può fornire i file di log in un unico bucket Amazon Simple Storage Service (Amazon S3) consolidato.

Puoi configurare più trail in modo tale che elaborino e registrino solo gli eventi specificati. Ciò può essere utile quando desideri eseguire il triage degli eventi che si verificano nel tuo Account AWS con gli eventi che si verificano nella tua applicazione.

> **Note**
>
> Per determinare se un file di log è stato modificato, eliminato o modificato dopo che CloudTrail lo ha distribuito, puoi utilizzare la funzionalità di convalida. Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende impossibile, a livello di programmazione, qualsiasi operazione di modifica, eliminazione o contraffazione dei file di log di CloudTrail senza che tale operazione venga rilevata. Puoi utilizzare la AWS CLI per convalidare i file nel percorso

in cui CloudTrail li ha distribuiti. Per ulteriori informazioni su questa funzionalità e su come abilitarla, consulta Convalida dell'integrità dei file di log di CloudTrail (documentazione di CloudTrail).

Casi d'uso per CloudTrail

- Aiuto per la conformità: l'utilizzo di CloudTrail può aiutarti a rispettare le policy interne e gli standard normativi fornendo una cronologia degli eventi nel tuo Account AWS.
- Analisi di sicurezza: puoi eseguire analisi di sicurezza e rilevare i modelli di comportamento degli utenti inserendo i file di log di CloudTrail in soluzioni di gestione e analisi dei log, come CloudWatch Logs, Amazon EventBridge, Amazon Athena, servizio OpenSearch di Amazon o un'altra soluzione di terze parti.
- Esfiltrazione di dati: è possibile rilevare l'esfiltrazione di dati raccogliendo dati sulle attività degli oggetti Amazon S3 tramite eventi API a livello di oggetto registrati in CloudTrail. Dopo aver raccolto i dati sull'attività, è possibile utilizzare altri Servizi AWS, come EventBridge e AWS Lambda, per attivare una risposta automatica.
- Risoluzione dei problemi operativi: è possibile risolvere i problemi operativi utilizzando i file di log di CloudTrail. Ad esempio, è possibile identificare rapidamente le modifiche più recenti apportate alle risorse del proprio ambiente, tra cui la creazione, la modifica e l'eliminazione di risorse AWS.

Best practice per CloudTrail

- Abilita CloudTrail in tutte le Regioni AWS.
- Abilita la convalida dell'integrità dei file di log.
- Crittografa i log.
- Inserisci i file di log di CloudTrail in CloudWatch Logs.
- Centralizza i log di tutti gli Account AWS e le regioni.
- Applica le policy del ciclo di vita ai bucket S3 contenenti file di log.
- Impedisci agli utenti di disattivare la registrazione in CloudTrail. Applica la seguente policy di controllo dei servizi (SCP) in AWS Organizations. Questo SCP imposta una regola di rifiuto esplicita per le azioni `StopLogging` e `DeleteTrail` in tutta l'organizzazione.

```
{
```

```
"Version": "2012-10-17",
"Statement":
       [
                 { "Action":
                     [
                     "cloudtrail:StopLogging",
                     "cloudtrail:DeleteTrail"
                      ],
                      "Resource": "*",
                      "Effect": "Deny"
                  }
        ]
}
```

Registrazione e monitoraggio delle applicazioni tramite Amazon CloudWatch

Amazon CloudWatch monitora le risorse AWS e le applicazioni che esegui su AWS in tempo reale. Puoi utilizzare CloudWatch per raccogliere e tenere traccia dei parametri, che sono delle variabili che si possono misurare per le risorse e le applicazioni.

Uso di CloudWatch

CloudWatch è essenzialmente un repository di parametri. Un Servizio AWS, ad esempio Amazon EC2, salva i parametri nel repository. Sulla base di questi parametri puoi recuperare le statistiche. Puoi anche recuperare le statistiche basate su questi parametri, se questi sono stati salvati nel repository. Per ulteriori informazioni, consulta Utilizzo dei parametri di CloudWatch (documentazione di CloudWatch).

Puoi anche configurare allarmi, che avviano automaticamente le azioni per tuo conto. Un allarme controlla un singolo parametro in un periodo di tempo specificato ed esegue una o più operazioni specificate in base al valore del parametro relativo a una determinata soglia durante un periodo di tempo. Ad esempio, un allarme può inviare una notifica a un argomento Amazon Simple Notification Service (Amazon SNS). Puoi anche aggiungere allarmi ai pannelli di controllo. Per ulteriori informazioni, consulta Utilizzo di allarmi CloudWatch (documentazione di CloudWatch).

La console di CloudWatch visualizza automaticamente i parametri relativi a ogni Servizio AWS utilizzato. Puoi creare pannelli di controllo aggiuntivi e personalizzati per visualizzare parametri e

allarmi per le tue applicazioni. Per ulteriori informazioni consulta Utilizzo dei pannelli di controllo di CloudWatch (documentazione di CloudWatch).

CloudWatch supporta automaticamente la funzionalità tra regioni. Non è necessario eseguire alcuna procedura aggiuntiva per visualizzare i parametri di diverse Regioni AWS in un singolo account sullo stesso grafico o sullo stesso pannello di controllo. È possibile ottenere la funzionalità tra account implementando osservabilità tra account (documentazione di CloudWatch).

Per ulteriori informazioni e linee guida dettagliate sull'utilizzo di CloudWatch per registrare e monitorare i carichi di lavoro nel Cloud AWS, consulta Progettazione e implementazione di registrazione e monitoraggio con Amazon CloudWatch (Prontuario di AWS).

Casi d'uso per CloudWatch

- Monitoraggio dell'integrità dell'applicazione: CloudWatch ServiceLens migliora l'osservabilità dei servizi e delle applicazioni abilitando l'integrazione di tracce, parametri, log, allarmi e altre informazioni sull'integrità delle risorse in un'unica posizione. ServiceLens integra CloudWatch con AWS X-Ray per fornire una panoramica completa dell'applicazione ed evidenziare in modo più efficiente i colli di bottiglia delle prestazioni e identificare gli utenti interessati. Per ulteriori informazioni, consulta Utilizzo di ServiceLens per monitorare l'integrità delle applicazioni (documentazione di CloudWatch).
- Monitoraggio sintetico: è possibile utilizzare CloudWatch Synthetics per creare canary e script configurabili eseguiti secondo una pianificazione, per monitorare endpoint e API. I canary seguono gli stessi percorsi ed eseguono le stesse azioni di un cliente, il che ti consente di verificare continuamente la tua esperienza cliente anche quando non hai alcun traffico clienti sulle tue applicazioni. I canary controllano la disponibilità e la latenza degli endpoint e possono archiviare i dati relativi al tempo di caricamento e le schermate dell'interfaccia utente. Monitorano le REST API, gli URL e il contenuto del sito Web e possono verificare le modifiche non autorizzate da phishing, code injection e cross-site scripting. Per ulteriori informazioni, consulta Utilizzo del monitoraggio sintetico (documentazione di CloudWatch).
- Monitoraggio utenti: con CloudWatch RUM, è possibile eseguire un monitoraggio reale degli utenti per raccogliere e visualizzare i dati lato client sulle prestazioni delle applicazioni Web. I dati includono tempo di caricamento delle pagine, errori lato client e comportamento dell'utente. È possibile utilizzare i dati raccolti per identificare ed eseguire rapidamente il debug dei problemi di prestazioni lato client. Per ulteriori informazioni, consulta Utilizzo di CloudWatch RUM (documentazione di CloudWatch).

- Rilevamento dei comportamenti anonimi: quando abiliti il rilevamento delle anomalie per un parametro, CloudWatch applica gli algoritmi statistici e di machine learning. Questi algoritmi analizzano continuamente i parametri di sistemi e applicazioni, determinano le normali linee di base e le anomalie superficiali. Per ulteriori informazioni, consulta Utilizzo del rilevamento delle anomalie di CloudWatch (documentazione di CloudWatch).
- Convalida di funzionalità ed esperimenti A/B: puoi utilizzare Amazon CloudWatch Evidently per convalidare in modo sicuro le nuove funzionalità servendole a una determinata percentuale di utenti durante il lancio della funzionalità. È inoltre possibile condurre esperimenti A/B per prendere decisioni sulla progettazione delle caratteristiche basate su prove e dati. Per ulteriori informazioni, consulta Esegui lanci ed esperimenti A/B con CloudWatch Evidently (documentazione di CloudWatch).

Registrazione e monitoraggio delle applicazioni tramite File di log Amazon CloudWatch

File di log Amazon CloudWatch consente di centralizzare i log da tutti i sistemi, le applicazioni e i Servizi AWS utilizzati in un unico servizio altamente scalabile. È quindi possibile visualizzarli facilmente, ricercarli per codici di errore o modelli specifici, filtrarli in base a campi specifici o archiviarli in modo sicuro per analisi future. Puoi visualizzare tutti gli eventi di log, indipendentemente dalla loro origine, come un flusso unico e coerente di eventi ordinati in base al tempo. Puoi interrogarli e ordinarli, raggrupparli per campi specifici, creare calcoli personalizzati e visualizzare i dati di log nei pannelli di controllo.

Utilizzo di CloudWatch Logs

In CloudWatch Logs, gli eventi di log sono organizzati in flussi di log e gruppi di log. Un flusso di log è una sequenza di eventi di log che condividono la stessa origine. Più precisamente, un flusso di log in genere è destinato a rappresentare la sequenza di eventi provenienti dall'istanza dell'applicazione o dalla risorsa monitorata. I gruppi di log definiscono uno o più flussi di log che condividono le stesse impostazioni di conservazione, monitoraggio e controllo degli accessi. Ogni flusso di log deve appartenere a un gruppo di log. Per ulteriori informazioni, consulta Utilizzo di gruppi di log e flussi di log (documentazione di CloudWatch Logs).

Puoi utilizzare CloudWatch Logs Insights per eseguire ricerche e analizzare i dati di log in File di log Amazon CloudWatch. Puoi eseguire le query per rispondere in modo rapido ed efficiente a problemi operativi. Se si verifica un problema, puoi utilizzare Logs Insights di CloudWatch per identificare

potenziali cause e convalidare le correzioni implementate. Per ulteriori informazioni consulta Analisi dei dati di log con CloudWatch Logs Insights (documentazione di CloudWatch Logs).

È possibile cercare e filtrare i dati di log che entrano in CloudWatch Logs creando uno o più filtri di parametri. I filtri di parametri definiscono i termini e i modelli per ricercare nei dati di log nel momento in cui si inviano a CloudWatch Logs. CloudWatch Logs utilizza queste filtri di parametri per trasformare i dati di log in parametri numerici di CloudWatch che puoi rappresentare graficamente o nei quali puoi impostare un allarme. Per ulteriori informazioni, consulta Creazione di parametri da eventi di log mediante filtri (documentazione di CloudWatch Logs).

Casi d'uso per CloudWatch Logs

- Monitoraggio di log di CloudTrail: puoi creare allarmi in CloudWatch e ricevere notifiche di una determinata attività dell'API acquisita da CloudTrail e utilizzare la notifica per eseguire la risoluzione dei problemi. Per ulteriori informazioni, consulta Invio di eventi CloudTrail in CloudWatch Logs (documentazione di CloudTrail).
- Registrazione di chiamate API AWS: se disponi di una soluzione di monitoraggio di terze parti, puoi utilizzare CloudWatch Logs per la registrazione di chiamate API AWS. Il servizio di monitoraggio di terze parti viene configurato per valutare questo log e le API a livello di applicazione.
- Configurazione della conservazione dei log: per impostazione predefinita, i log in CloudWatch Logs vengono conservati a tempo indeterminato e non scadono mai. Puoi modificare la policy di conservazione per ogni gruppo di log mantenendo la conservazione a tempo indeterminato o scegliendo periodi di conservazione compresi tra un giorno e 10 anni.
- Archiviazione e memorizzazione dei log: è possibile utilizzare CloudWatch Logs per memorizzare i dati di log in un sistema di storage a lunga durata. L'agente di CloudWatch Logs invia dati di log ruotati e non ruotati nel servizio di log. Puoi quindi accedere ai dati di log grezzi in caso di necessità.

Registrazione e monitoraggio di applicazioni tramite Log di flusso VPC

Log di flusso VPC è una funzionalità di Amazon Virtual Private Cloud (Amazon VPC) che consente di acquisire informazioni sul traffico IP da e verso le interfacce di rete nel VPC.

Utilizzo di Log di flusso VPC

Puoi creare un log di flusso per un cloud virtuale privato (VPC), una sottorete o un'interfaccia di rete. Se crei un log di flusso per una sottorete o un VPC, viene monitorata ogni interfaccia di rete nella sottorete o nel VPC. Per ulteriori informazioni, consulta Utilizzo dei log di flusso (documentazione di Amazon VPC).

I dati di log di flusso in un'interfaccia di rete monitorata vengono registrati come record di log di flusso. Un record di log di flusso rappresenta un flusso di rete nel VPC. Per impostazione predefinita, ogni record acquisisce un flusso di traffico IP di rete che si verifica all'interno di un intervallo di aggregazione. Ogni record è una stringa con campi separati da spazi. Un record include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo. Quando crei un log di flusso, puoi utilizzare il formato predefinito oppure specificare un formato personalizzato. Per ulteriori informazioni, consulta Esempi di record di log di flusso (documentazione di Amazon VPC).

I log di flusso non acquisiscono le seguenti informazioni:

- Traffico generato da istanze quando contattano il server del sistema dei nomi di dominio (DNS) Amazon. Se si utilizza il proprio server DNS, tutto il traffico al server DNS viene registrato.
- Traffico generato da un'istanza Windows per attivazione licenza Windows Amazon.
- Traffico da e verso `254.169.254` per metadati di istanza.
- Traffico da e verso `254.169.123` per il servizio di sincronizzazione oraria di Amazon.
- Traffico del protocollo di configurazione per host dinamico (DHCP).
- Traffico all'indirizzo IP riservato per il router VPC predefinito.
- Traffico tra un'interfaccia di rete endpoint e un'interfaccia di rete Network Load Balancer.

I dati del log di flusso possono essere pubblicati in vari Servizi AWS, incluso File di log Amazon CloudWatch. Dopo aver creato un log di flusso, puoi recuperare e visualizzare i record del log di flusso in CloudWatch Logs, nel gruppo di log configurato. Per ulteriori informazioni, consulta Pubblica i log di flusso in CloudWatch Logs (documentazione di Amazon VPC).

I dati di log del flusso vengono raccolti al di fuori del percorso del traffico di rete e pertanto non influiscono sulla velocità effettiva o sulla latenza della rete. È possibile creare o eliminare i log di flusso senza alcun rischio di impatto sulle prestazioni della rete.

Casi d'uso per Log di flusso VPC

- Diagnosi di regole del gruppo di sicurezza eccessivamente restrittive
- Monitoraggio del traffico che raggiunge l'istanza dell'applicazione
- Determinazione della direzione del traffico

Registrazione e monitoraggio di applicazioni tramite AWS X-Ray

AWS X-Ray raccoglie i dati sulle richieste gestite dall'applicazione e consente di visualizzare, filtrare e analizzare i dati per identificare i problemi e le opportunità di ottimizzazione.

Utilizzo di X-Ray

AWS X-Ray riceve tracce dalla tua applicazione e, se sono integrate con X-Ray, dai Servizi AWS utilizzati dalla tua applicazione. X-Ray campiona e visualizza le richieste su un grafico di servizio quando fluiscono attraverso i componenti dell'applicazione. X-Ray genera identificatori di traccia in modo da poter correlare una richiesta quando fluisce attraverso più componenti, il che consente di visualizzare la richiesta dall'inizio alla fine. È possibile migliorare ulteriormente questa funzionalità includendo annotazioni e metadati per aiutare a cercare e identificare in modo univoco le caratteristiche di una richiesta.

Si consiglia di configurare ogni server o endpoint dell'applicazione con X-Ray. X-Ray viene implementato nel codice dell'applicazione effettuando chiamate al servizio X-Ray. X-Ray fornisca anche SDK AWS per più lingue, inclusi client strumentati che inviano automaticamente i dati a X-Ray. Gli SDK X-Ray forniscono patch alle librerie comuni utilizzate per effettuare chiamate ad altri servizi (ad esempio, HTTP, MySQL, PostgreSQL o MongoDB).

Per ulteriori informazioni, consulta Tracciamento di applicazioni conAWS X-Ray (Linee guida prescrittive di AWS).

Casi d'uso per X-Ray

- Analisi e debug di applicazioni: i dati di traccia possono aiutarti a eseguire il debug dell'applicazione fornendo una visione completa della richiesta in modo da poter identificare i punti deboli e risolvere i problemi. La mappa dei servizi di XRay è uno strumento visivo che consente di identificare dove si verificano gli errori, le connessioni con latenza elevata o le tracce delle richieste non riuscite.

- Analisi delle prestazioni: la console di analisi è uno strumento interattivo per interpretare i dati di traccia in modo da valutare rapidamente le prestazioni dell'applicazione e dei servizi sottostanti. La console ti aiuta a esplorare, analizzare e visualizzare le tracce. Puoi inoltre confrontare set di tracce con condizioni diverse, per l'analisi della causa principale.

Domande frequenti

Posso usare il mio servizio di monitoraggio attuale?

Amazon CloudWatch è un servizio di monitoraggio e osservabilità creato per ingegneri DevOps, sviluppatori, ingegneri dell'affidabilità del sito (SRE), responsabili IT e proprietari di applicazioni. Fornisce dati e analisi concrete per monitorare le applicazioni e rispondere ai cambiamenti di prestazioni a livello di sistema e ottimizzare l'utilizzo delle risorse. Tuttavia, se disponi di un servizio di monitoraggio consolidato, non è necessario sostituirlo.

Come posso impedire che i file di log vengano manomessi?

Puoi abilitare la convalida dell'integrità dei file di log. È buona norma gestire e archiviare i log in un Account AWS dedicato e limitare l'accesso a quell'account. Per ulteriori informazioni sul tagging, consulta Utilizzo di CloudTrail in questa guida.

Devo mantenere file di log separati per ogni applicazione?

No, puoi consolidare i dati di log di più applicazioni nello stesso file di log. Tuttavia, assicurati che nel flusso di log sia registrato un identificatore univoco per ogni applicazione.

Risorse

Documentazione AWS

- Documentazione di AWS CloudTrail
- Documentazione Cloud AWSWatch
- Documentazione Cloud AWSWatch Logs
- Documentazione su Log di flusso Amazon VPC
- Documentazione di AWS X-Ray
- Progettazione e implementazione di registrazione e monitoraggio con Amazon CloudWatch (Prontuario di AWS)

Marketing AWS

- AWS CloudTrail
- Amazon CloudWatch
- Registrazione centralizzata su AWS (Soluzioni AWS)
- Monitoraggio e osservabilità (Operazioni Cloud AWS)
- Come monitorare le applicazioni in modo efficace (Avvio di AWS)

Cronologia dei documenti

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

Modifica	Descrizione	Data
Pubblicazione iniziale	—	6 gennaio 2023

AWS Glossario delle linee guida prescrittive

I seguenti sono termini comunemente usati 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 di 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 aggregata

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

Il processo di utilizzo delle tecniche di machine learning per risolvere problemi operativi, ridurre gli incidenti operativi e l'intervento umano e aumentare la qualità del servizio. Per ulteriori informazioni su come viene utilizzato AIOps nella strategia di migrazione AWS , consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

Un bot che ha lo scopo di 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.

distribuzioni blu/verdi

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 AWS Cloud Adoption 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.

CoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

centro di eccellenza del cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

Queste fasi sono state definite da Stephen Orban nel post del blog The Journey Toward Cloud-First & the Stages of Adoption 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 o AWS CodeCommit. 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, AWS Panorama offre dispositivi che aggiungono CV alle reti di telecamere locali e Amazon SageMaker 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, creazione, test, gestione temporanea e produzione del processo di rilascio del software. Il processo CI/CD è comunemente descritto come una

pipeline. CI/CD può aiutare ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le distribuzioni. 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.

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.

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 pipeline CI/CD, l'ambiente di produzione è l'ultimo ambiente di implementazione.
- 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 la 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, vedere 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.

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.

G

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.

strategia greenfield

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

guardrail

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

I

IaC

Considera 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. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

Internet delle cose industriale (IIoT)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

Una caratteristica di un modello di machine learning che descrive il grado in cui un essere umano è in grado di comprendere in che modo le previsioni del modello dipendono dai suoi input. Per ulteriori informazioni, consulta la sezione Interpretabilità dei modelli 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.

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.

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

Un AWS programma che fornisce consulenza, supporto, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

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

fabbrica di migrazione

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione a. Cloud AWS MPA offre una valutazione dettagliata del portfolio (dimensionamento

corretto dei server, prezzi, confronto del TCO, analisi dei costi di migrazione) e pianificazione della migrazione (analisi e raccolta dei dati delle applicazioni, raggruppamento delle applicazioni, prioritizzazione delle migrazioni e pianificazione delle ondate). Lo strumento MPA (richiede l'accesso) è disponibile gratuitamente per tutti i AWS consulenti e i consulenti dei partner APN.

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

Applicazioni eseguite come un unico servizio con processi strettamente collegati. Le applicazioni monolitiche presentano diversi inconvenienti. Se una funzionalità dell'applicazione registra un

picco di domanda, l'intera architettura deve essere dimensionata. L'aggiunta o il miglioramento delle funzionalità di un'applicazione monolitica diventa inoltre più complessa man mano che la base di codice cresce. Per risolvere questi problemi, puoi utilizzare un'architettura di microservizi. Per ulteriori informazioni, consulta la sezione Scomposizione dei monoliti in microservizi.

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

Un percorso creato da noi AWS CloudTrail che registra tutti gli eventi di un'organizzazione per tutti Account AWS . AWS Organizations Questo percorso viene creato in ogni Account AWS che fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione nella CloudTrail documentazione.

gestione del cambiamento organizzativo (OCM)

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

O

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

In un'architettura AWS multi-account, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

Privacy fin dalla progettazione

Un approccio all'ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di progettazione.

zone ospitate private

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

controllo proattivo

Un controllo di sicurezza progettato per impedire l'implementazione di risorse non conformi. Questi controlli analizzano le risorse prima del loro provisioning. Se la risorsa non è conforme al controllo, non viene fornita. Per ulteriori informazioni, consulta la guida di riferimento sui controlli nella AWS Control Tower documentazione e consulta Controlli proattivi in Implementazione dei controlli di sicurezza su. AWS

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

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.

pubblica/sottoscrivi (pub/sub)

Un pattern 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).

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 il 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. Ciò determina quella che viene considerata 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.

Regione

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

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

La capacità di un'applicazione di resistere o ripristinare le interruzioni. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud 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.

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 l'obiettivo del punto di ripristino.

RTO

Vedi l'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 AWS Management Console 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 AWS Secrets Manager, 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.

controllo di sicurezza

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

rafforzamento della sicurezza

Il processo di riduzione della superficie di attacco per renderla più resistente agli attacchi. Può includere azioni come la rimozione di risorse che non sono più necessarie, l'implementazione di

best practice di sicurezza che prevedono la concessione del privilegio minimo o la disattivazione di funzionalità non necessarie nei file di configurazione.

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

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

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

Una metrica target che rappresenta lo stato di un servizio, misurato da un indicatore del livello di servizio.

Modello di responsabilità condivisa

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

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.

T

tags

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 è possibile utilizzare per collegare i VPC e le reti on-premise. Per ulteriori informazioni, consulta Cos'è un gateway di transito nella AWS Transit Gateway documentazione.

flusso di lavoro basato su trunk

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

Accesso attendibile

Concessione delle autorizzazioni a un servizio specificato dall'utente per eseguire attività all'interno dell'organizzazione AWS Organizations e nei suoi account per conto dell'utente. Il servizio attendibile crea un ruolo collegato al servizio in ogni account, quando tale ruolo è necessario, per eseguire attività di gestione per conto dell'utente. Per ulteriori informazioni,

consulta Utilizzo AWS Organizations con altri AWS servizi nella AWS Organizations documentazione.

regolazione

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

team da due pizze

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

U

incertezza

Un concetto che si riferisce a informazioni imprecise, incomplete o sconosciute che possono minare l'affidabilità dei modelli di machine learning predittivi. Esistono due tipi di incertezza: l'incertezza epistemica, che è causata da dati limitati e incompleti, mentre l'incertezza aleatoria è causata dal rumore e dalla casualità insiti nei dati. 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 VPC che consente di instradare il traffico tramite indirizzi IP privati. Per ulteriori informazioni, consulta Che cos'è il peering VPC? nella documentazione di Amazon VPC.

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

Gruppi funzionali in un progetto di migrazione responsabili di una serie specifica di attività. Ogni flusso di lavoro è indipendente ma supporta gli altri flussi di lavoro del progetto. Ad esempio,

il flusso di lavoro del portfolio è responsabile della definizione delle priorità delle applicazioni, della pianificazione delle ondate e della raccolta dei metadati di migrazione. Il flusso di lavoro del portfolio fornisce queste risorse al flusso di lavoro di migrazione, che quindi migra i server e le applicazioni.

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

Un attacco, in genere malware, che sfrutta una vulnerabilità zero-day.

vulnerabilità zero-day

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

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.