Strumenti e best practice di monitoraggio e invio di avvisi per Amazon RDS for My SQL e MariaDB

AWS Guida prescrittiva

AWS Guida prescrittiva: Strumenti e best practice di monitoraggio e invio di avvisi per Amazon RDS for My SQL e MariaDB

Table of Contents

Strumenti e best practice di monitoraggio e invio di avvisi per Amazon RDS for MySQL e MariaDB

Igor Obradovic, Amazon Web Services ()AWS

Giugno 2024 (cronologia del documento)

Il monitoraggio del database è il processo di misurazione, tracciamento e valutazione della disponibilità, delle prestazioni e della funzionalità di un database. Le soluzioni di monitoraggio e avviso aiutano le organizzazioni a garantire che i servizi di database, e quindi le applicazioni e i carichi di lavoro associati, siano sicuri, ad alte prestazioni, resilienti ed efficienti. Su AWS, puoi raccogliere e analizzare i log, le metriche, gli eventi e le tracce del carico di lavoro per comprendere lo stato del tuo carico di lavoro e ottenere informazioni dettagliate dalle operazioni nel tempo.

Puoi monitorare le tue risorse per assicurarti che funzionino come previsto e per rilevare e risolvere eventuali problemi prima che abbiano un impatto sui tuoi clienti. È necessario utilizzare le metriche, i log, gli eventi e le tracce monitorati per generare allarmi in caso di superamento delle soglie.

Questa guida descrive gli strumenti di osservabilità e monitoraggio dei database e le best practice per i database Amazon Relational Database Service (Amazon RDS). La guida si concentra sui database MySQL e MariaDB, sebbene la maggior parte delle informazioni si applichi anche ad altri motori di database Amazon RDS.

Questa guida è per architetti di soluzioni, architetti di database, DBA, DevOps ingegneri senior e altri membri del team impegnati nella progettazione, implementazione e gestione di soluzioni di monitoraggio e osservabilità per i carichi di lavoro di database in esecuzione nel cloud AWS.

Indice

- Passaggi e risorse successivi

Panoramica

Il monitoraggio e gli avvisi sono inclusi nei quattro pilastri del Well-Architected AWS Framework.

- Il pilastro dell'eccellenza operativa prescrive che il carico di lavoro sia progettato per includere telemetria e monitoraggio. AWS servizi come Amazon Relational Database Service (Amazon RDS) forniscono le informazioni necessarie per comprendere lo stato interno del carico di lavoro (ad esempio metriche, log, eventi e tracce). Quando gestisci i tuoi database Amazon RDS, vorrai conoscere lo stato delle istanze dei database, rilevare eventi operativi ed essere in grado di rispondere a eventi pianificati e non pianificati. AWS fornisce strumenti di monitoraggio che ti aiutano a determinare quando i risultati organizzativi e di business sono a rischio, o potenzialmente potrebbero esserlo, in modo da poter intraprendere le azioni appropriate al momento giusto.
- Il pilastro dell'efficienza delle prestazioni prescrive di monitorare le prestazioni delle risorse, come le istanze database di Amazon RDS, raccogliendo, aggregando ed elaborando i parametri relativi alle prestazioni in tempo reale. Puoi identificare il peggioramento delle prestazioni e porre rimedio ai fattori che lo hanno causato, ad esempio, query SQL non ottimizzate o parametri di configurazione inadeguati. È possibile generare allarmi automaticamente quando le misurazioni superano i limiti previsti. Ti consigliamo di utilizzare gli allarmi non solo per le notifiche, ma anche per avviare azioni automatiche in risposta agli eventi rilevati. Puoi valutare le metriche raccolte rispetto a soglie predefinite o utilizzare algoritmi di apprendimento automatico per identificare comportamenti anomali. Ad esempio, per rilevare una tendenza all'aumento dell'utilizzo della CPU, puoi raccogliere e analizzare la metrica per un periodo di tempo. `cpuUtilization.total` La segnalazione proattiva di tale anomalia, prima che l'utilizzo della CPU raggiunga il limite massimo, può aiutarvi a risolvere il problema prima che si ripercuota sui clienti.
- Il pilastro dell'affidabilità definisce il monitoraggio e l'invio di avvisi come elementi fondamentali per garantire il rispetto dei requisiti di disponibilità. La soluzione di monitoraggio deve essere in grado di rilevare i guasti in modo efficace. Quando rileva problemi o guasti, il suo obiettivo principale è quello di avvisare su tali problemi. L'implementazione di pratiche di osservabilità e monitoraggio continue è fondamentale per le architetture resilienti nel cloud. Per migliorare i carichi di lavoro, devi essere in grado di misurarli e comprenderne lo stato e lo stato di salute. I principi di progettazione per il ripristino automatico in caso di guasto, la scalabilità orizzontale e il provisioning della capacità dipendono da servizi di monitoraggio e avviso accurati.
- Il pilastro della sicurezza riguarda il rilevamento e la prevenzione di modifiche di configurazione impreviste o indesiderate e di comportamenti imprevisti. Puoi configurare le tue istanze Amazon RDS for MySQL e MariaDB DB con il MariaDB Audit Plugin per registrare le attività del database,

come gli accessi degli utenti e le operazioni specifiche eseguite sul database. Il plug-in memorizza il record dell'attività del database in un file di registro, che può essere integrato e importato in strumenti di monitoraggio e avviso. Il file di registro viene analizzato in tempo reale per rilevare eventuali comportamenti imprevisti o sospetti nel database. Tale comportamento imprevisto o sospetto può indicare che la tua istanza database Amazon RDS è stata compromessa, il che segnala potenziali rischi per la tua azienda. Se lo strumento di monitoraggio rileva un evento del genere, attiva un allarme per avviare una risposta all'incidente di sicurezza, che aiuta a risolvere attività sospette e dannose.

Obiettivi aziendali specifici

L'implementazione delle migliori pratiche nei meccanismi di monitoraggio e avviso aiuta a garantire un'infrastruttura ad alte prestazioni, resiliente, efficiente, sicura e ottimizzata in termini di costi per le applicazioni e i carichi di lavoro. È possibile utilizzare strumenti di osservabilità che raccolgono, archiviano e visualizzano metriche, eventi, tracce e registri in tempo reale per osservare e analizzare il quadro più ampio dello stato e delle prestazioni dei database e quindi prevenire il degrado o l'interruzione dei servizi IT associati. Se si verifica ancora un degrado non pianificato o un'interruzione del servizio, gli strumenti di monitoraggio e avviso aiutano a rilevare tempestivamente il problema, l'aggravamento, la reazione e a indagare e risolvere rapidamente. Una soluzione completa di monitoraggio e avviso per i carichi di lavoro del database cloud ti aiuta a raggiungere i seguenti risultati aziendali:

- Migliora l'esperienza dei clienti. Un servizio affidabile migliora l'esperienza dei tuoi clienti. I database sono spesso un componente chiave di servizi digitali come applicazioni web e mobili, streaming multimediale, pagamenti, API business-to-business (B2B) e servizi di integrazione. Se riesci a monitorare e impostare avvisi sui tuoi database per rilevare rapidamente i problemi, analizzarli in modo efficiente e correggerli il prima possibile per ridurre al minimo i tempi di inattività e altre interruzioni, puoi migliorare la disponibilità, la sicurezza e le prestazioni del servizio digitale per i tuoi clienti.
- Costruisci la fiducia dei clienti.Prestazioni migliori e un'esperienza utente più fluida ti aiutano a conquistare la fiducia dei tuoi clienti, il che può tradursi in un aumento del business sulla tua piattaforma. Ad esempio, un fornitore di servizi di elaborazione dei pagamenti che offre un servizio online affidabile può aspettarsi un'elevata fiducia e fidelizzazione dei clienti, il che si traduce in un maggior numero di clienti e una migliore fidelizzazione, un aumento delle transazioni fatturabili e servizi nuovi e innovativi che generano maggiori entrate.

- Evita perdite finanziarie.Qualsiasi downtime imprevisto dell'infrastruttura di database può influire sulle transazioni commerciali eseguite dai clienti utilizzando l'applicazione. In alcuni casi, ciò può portare a perdite finanziarie considerevoli. La violazione degli accordi sui livelli di servizio (SLA) potrebbe comportare la perdita della fiducia dei clienti e, di conseguenza, una perdita di ricavi. Può anche diventare una base legale per costosi processi, in cui i clienti potrebbero richiedere un risarcimento in base ai contratti di responsabilità e garanzia stipulati. Secondo uno studio condotto da Atlassian Corporation, una società di software, i costi medi di interruzione del servizio sono compresi tra 140 mila dollari e 540.000 dollari all'ora, a seconda del tipo e delle dimensioni dell'azienda. Un ambiente di database stabile è fondamentale per prevenire interruzioni prolungate e perdite di attività.
- Espandi il valore. I meccanismi di monitoraggio e avviso possono aiutarti a progettare, sviluppare e gestire un servizio digitale altamente disponibile, resiliente, affidabile, performante, conveniente e sicuro, ma è solo l'inizio. Desideri che la tua organizzazione cresca e cresca nel tempo, migliori i carichi di lavoro cloud esistenti e introduca nuovi servizi. I nuovi servizi offrono valore aggiunto ai tuoi clienti e maggiori entrate alla tua azienda, creando un effetto volano sulla crescita della tua attività.
- Migliora la produttività degli sviluppatori.Gli sviluppatori che sono produttivi ed efficienti e che non incontrano problemi e rallentamenti nelle loro attività di sviluppo, possono fornire prodotti di alta qualità in tempi più brevi. Tuttavia, l'ingegneria del software e le operazioni IT spesso presentano sfide complesse e tale complessità aumenta con la scala dei carichi di lavoro e delle relative architetture. Per analizzare le prestazioni e la coerenza tra le applicazioni distribuite, gli sviluppatori necessitano di strumenti in grado di fornire metriche e tracce correlate. Questi aiutano a identificare gli artefatti di codice e i componenti dell'infrastruttura difettosi il più rapidamente possibile e aiutano a determinare gli impatti sugli utenti finali. La giusta suite di strumenti di monitoraggio e avviso può aiutare gli sviluppatori a programmare e testare meglio e più velocemente.
- Migliora l'efficacia e l'efficienza operativa.Quando gestisci carichi di lavoro cloud su larga scala, anche una piccola percentuale di miglioramenti delle prestazioni può portare a risparmi per milioni di dollari. Monitorando i tuoi database e analizzando metriche, eventi, log e tracce, puoi comprendere e prevedere le tue future esigenze di capacità e sfruttare i risparmi sui costi disponibili nel cloud AWS. Comprendere i carichi di lavoro e lo stato operativo di Amazon RDS può aiutarti a rispondere agli eventi, risolvere problemi e pianificare miglioramenti.

Procedure consigliate generali

Le seguenti best practice ti aiutano a ottenere una visibilità sufficiente sullo stato del tuo carico di lavoro Amazon RDS e a intraprendere le azioni appropriate in risposta agli eventi operativi e al monitoraggio dei dati.

- Identifica i KPI.Identifica gli indicatori chiave di performance (KPI) in base ai risultati aziendali desiderati. Valuta i KPI per determinare il successo del carico di lavoro. Ad esempio, se la tua attività principale è l'e-commerce, uno dei risultati commerciali che desideri potrebbe essere che il tuo e-shop sia disponibile 24 ore su 24, 7 giorni su 7, per consentire ai tuoi clienti di fare acquisti. Per ottenere questo risultato aziendale, definisci il KPI di disponibilità per il database di backend Amazon RDS utilizzato dall'applicazione di e-shop e imposti il KPI di base al 99,99% su base settimanale. La valutazione del KPI di disponibilità effettivo rispetto al valore di base consente di determinare se si soddisfa la disponibilità del database desiderata del 99,99% e quindi si ottiene il risultato aziendale di disporre di un servizio 24 ore su 24, 7 giorni su 7.
- Definisci le metriche del carico di lavoro.Definisci le metriche del carico di lavoro per misurare le quantità e le qualità del tuo carico di lavoro Amazon RDS. Valuta le metriche per determinare se il carico di lavoro sta ottenendo i risultati desiderati e per comprendere lo stato del carico di lavoro. Ad esempio, per valutare il KPI di disponibilità per la tua istanza database Amazon RDS, devi misurare metriche come i tempi di attività e i tempi di inattività dell'istanza database. Puoi quindi utilizzare queste metriche per calcolare il KPI di disponibilità come segue:

  ```
  availability = uptime / (uptime + downtime)
  ```

  Le metriche rappresentano set di punti dati ordinati nel tempo. Le metriche possono includere anche dimensioni, utili per la categorizzazione e l'analisi.
- Raccogli e analizza le metriche del carico di lavoro.Amazon RDS genera metriche e log diversi, a seconda della configurazione. Alcuni di questi rappresentano eventi, contatori o statistiche delle istanze di database, come`db.Cache.innoDB_buffer_pool_hits`. Altre metriche provengono dal sistema operativo, come`memory.Total`, che misura la quantità totale di memoria dell'istanza host di Amazon Elastic Compute Cloud (Amazon EC2). Lo strumento di monitoraggio dovrebbe eseguire un'analisi regolare e proattiva delle metriche raccolte per identificare le tendenze e determinare se sono necessarie risposte appropriate.
- Stabilisci delle baseline delle metriche del carico di lavoro.Stabilisci delle linee di base per le metriche per definire i valori attesi e identificare le soglie positive o negative. Ad esempio, è

possibile definire la linea di base per`ReadIOPS`fino a 1.000 con le normali operazioni del database. È quindi possibile utilizzare questa linea di base per il confronto e identificare un utilizzo eccessivo. Se le nuove metriche mostrano costantemente che gli IOPS in lettura sono compresi tra 2.000 e 3.000, hai identificato una deviazione che potrebbe innescare una risposta per l'indagine, l'intervento e il miglioramento.

- Avvisa quando i risultati del carico di lavoro sono a rischio.Quando stabilisci che il risultato aziendale è a rischio, invia un avviso. Puoi quindi affrontare i problemi in modo proattivo, prima che influiscano sui tuoi clienti, o mitigare l'impatto dell'incidente in modo tempestivo.
- Identifica i modelli di attività previsti per il tuo carico di lavoro.In base alle baseline delle tue metriche, stabilisci modelli di attività del carico di lavoro per identificare comportamenti imprevisti e rispondere con azioni appropriate, se necessario.AWSforniscestrumenti di monitoraggiochе applicano algoritmi statistici e di apprendimento automatico per analizzare le metriche e rilevare anomalie.
- Avvisa quando vengono rilevate anomalie del carico di lavoro.Quando vengono rilevate anomalie nelle operazioni dei carichi di lavoro di Amazon RDS, invia un avviso in modo da poter rispondere con le azioni appropriate, se necessario.
- Rivedi e rivedi i KPI e le metriche. Verifica che i tuoi database Amazon RDS soddisfino i requisiti definiti e identifica le aree di potenziale miglioramento per raggiungere i tuoi obiettivi aziendali. Convalida l'efficacia delle metriche misurate e dei KPI valutati e, se necessario, modificali. Ad esempio, supponiamo che tu imposti un KPI per il numero ottimale di connessioni simultanee al database e che controlli le metriche relative alle connessioni tentate e non riuscite e ai thread utente che sono stati creati e in esecuzione. Potresti avere più connessioni al database rispetto a quelle definite dalla tua linea di base KPI. Analizzando le tue metriche attuali, puoi rilevare il risultato ma potresti non essere in grado di determinare la causa principale. In tal caso, dovresti rivedere le tue metriche e includere misure di monitoraggio aggiuntive, come i contatori per le serrature dei tavoli. Le nuove metriche consentirebbero di determinare se l'aumento del numero di connessioni al database è causato da blocchi imprevisti delle tabelle.

Strumenti di monitoraggio

Ti consigliamo di utilizzare strumenti di osservabilità, monitoraggio e avviso per:

- Ottieni informazioni dettagliate sulle prestazioni del tuo ambiente Amazon RDS
- Rileva comportamenti imprevisti e sospetti
- Pianifica la capacità e prendi decisioni consapevoli sull'allocazione delle istanze Amazon RDS
- Analizza metriche e log per prevedere potenziali problemi in modo proattivo
- Genera avvisi quando vengono superate le soglie per risolvere e risolvere i problemi prima che gli utenti ne risentano

Hai diverse opzioni e soluzioni tra cui scegliere, tra cui strumenti e servizi di osservabilità e monitoraggio nativi del cloud forniti da AWS, soluzioni software gratuite e open source e soluzioni commerciali di terze parti per il monitoraggio delle istanze DB di Amazon RDS. Alcuni di questi strumenti sono descritti nelle sezioni che seguono.

Per determinare lo strumento più adatto alle tue esigenze, confronta le caratteristiche e le funzionalità di ogni strumento con i requisiti della tua organizzazione. Si consiglia inoltre di valutare gli strumenti per quanto riguarda la facilità di implementazione, configurazione e integrazione, gli aggiornamenti e la manutenzione del software, il metodo di distribuzione (ad esempio, hardware o serverless), le licenze, il prezzo e qualsiasi altro fattore specifico dell'organizzazione.

Sections

Strumenti inclusi in Amazon RDS

Amazon Relational Database Service (Amazon RDS) è un servizio di database gestito nel cloud AWS. Poiché Amazon RDS è un servizio gestito, ti libera dalla maggior parte delle attività di gestione, come backup del database, installazioni di sistemi operativi (OS) e software di database, patch di sistemi operativi e software, configurazione ad alta disponibilità, ciclo di vita dell'hardware e operazioni del data center. AWS fornisce inoltre un set completo di strumenti che consentono di creare una soluzione di osservabilità completa per le istanze database di Amazon RDS.

Alcuni strumenti di monitoraggio sono inclusi, preconfigurati e abilitati automaticamente nel servizio Amazon RDS. Due strumenti automatici sono disponibili non appena avvii la tua nuova istanza Amazon RDS:

- Lo stato dell'istanza Amazon RDS fornisce dettagli sullo stato attuale dell'istanza DB. Ad esempio, i codici di stato includono Available, Stopped, Creating, Backing-up e Failed. Puoi utilizzare la console Amazon RDS, il AWS Command Line Interface (AWS CLI) o l'API Amazon RDS per visualizzare lo stato dell'istanza. Per ulteriori informazioni, consulta Visualizzazione dello stato dell'istanza DB di Amazon RDS nella documentazione di Amazon RDS.
- I consigli di Amazon RDS forniscono consigli automatici per istanze DB, repliche di lettura e gruppi di parametri DB. Questi consigli vengono forniti analizzando l'utilizzo delle istanze DB, i dati prestazionali e la configurazione e vengono forniti come guida. Ad esempio, il consiglio relativo alla versione obsoleta di Engine suggerisce che le istanze DB non eseguono la versione più recente del software di database e che è necessario aggiornare l'istanza DB per beneficiare delle ultime correzioni di sicurezza e di altri miglioramenti. Per ulteriori informazioni, consulta Visualizzazione dei consigli di Amazon RDS nella documentazione di Amazon RDS.

CloudWatch namespace

Amazon RDS si integra con Amazon CloudWatch, un servizio di monitoraggio e avviso per risorse e applicazioni cloud eseguite su AWS. Amazon RDS raccoglie automaticamente parametri, file di log, tracce ed eventi relativi al funzionamento, all'utilizzo, alle prestazioni e allo stato delle istanze DB e li invia CloudWatch per lo storage, l'analisi e gli avvisi a lungo termine.

Amazon RDS for MySQL e Amazon RDS for MariaDB pubblicano automaticamente un set predefinito di parametri a intervalli di un minuto senza costi aggiuntivi. CloudWatch Queste metriche vengono raccolte in due namespace, che sono contenitori per metriche:

- Lo spazio dei nomi AWS/RDS include metriche a livello di istanza DB. Gli esempi includono `BinLogDiskUsage` (la quantità di spazio su disco occupato dai log binari), `CPUUtilization` (la percentuale di utilizzo della CPU), (il numero di connessioni di rete client all'`DatabaseConnections`istanza DB) e molti altri.
- Lo spazio dei nomi AWS/Usage include metriche di utilizzo a livello di account, che vengono utilizzate per determinare se stai operando entro le quote del servizio Amazon RDS. Gli esempi includono `DBInstances` (il numero di istanze DB nel tuo account o nella tua regione AWS), `DBSubnetGroups` (il numero di sottoreti DB nel tuo AWS account o nella tua regione) e `ManualSnapshots` (il numero di snapshot di database creati manualmente nel tuo AWS account o nella tua regione).

CloudWatch conserva i dati metrici come segue:

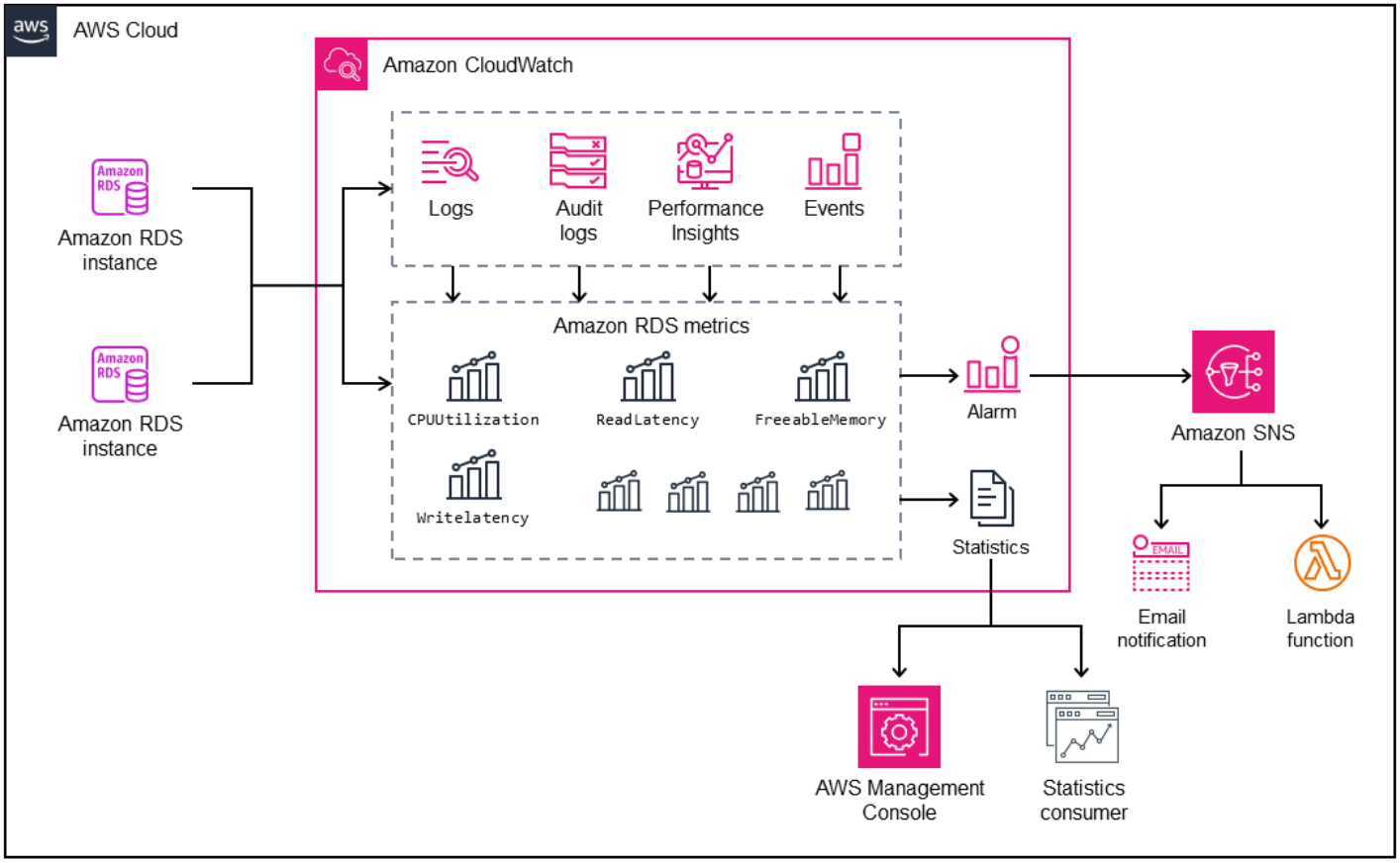
- 3 ore: le metriche personalizzate ad alta risoluzione con un periodo inferiore a 60 secondi vengono conservate per 3 ore. Dopo 3 ore, i punti dati vengono aggregati in metriche con periodo di 1 minuto e conservati per 15 giorni.
- 15 giorni: i punti dati con un periodo di 60 secondi (1 minuto) vengono conservati per 15 giorni. Dopo 15 giorni, i punti dati vengono aggregati in metriche con periodi di 5 minuti e conservati per 63 giorni.
- 63 giorni: i punti dati con un periodo di 300 secondi (5 minuti) vengono conservati per 63 giorni. Dopo 63 giorni, i punti dati vengono aggregati in metriche con periodo di 1 ora e conservati per 15 mesi.
- 15 mesi: i punti dati con un periodo di 3.600 secondi (1 ora) sono disponibili per 15 mesi (455 giorni).

Per ulteriori informazioni, consulta Metriche nella documentazione. CloudWatch

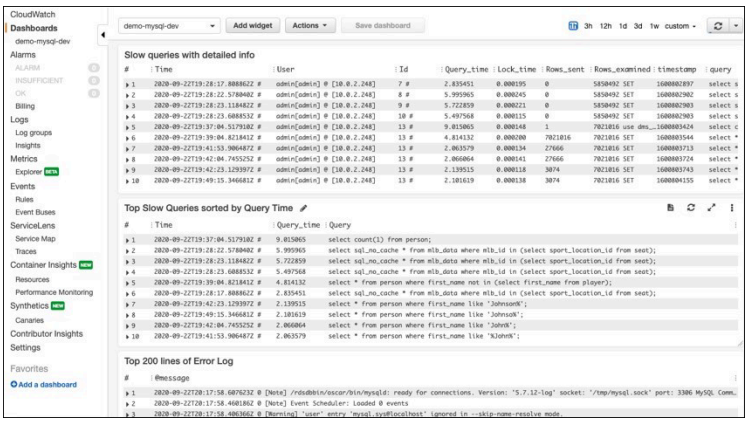
CloudWatch allarmi e dashboard

Puoi utilizzare Amazon CloudWatch Alarms per monitorare una metrica Amazon RDS specifica per un periodo di tempo. Ad esempio, puoi monitorare `FreeStorageSpace` e quindi eseguire una o più azioni se il valore della metrica supera la soglia impostata. Se imposti la soglia su 250 MB e lo spazio di archiviazione libero è di 200 MB (inferiore alla soglia), l'allarme verrà attivato e può attivare un'azione per fornire automaticamente spazio di archiviazione aggiuntivo per l'istanza database di

Amazon RDS. L'allarme può anche inviare un SMS di notifica al DBA utilizzando Amazon Simple Notification Service (Amazon SNS). Il diagramma seguente illustra tale processo.

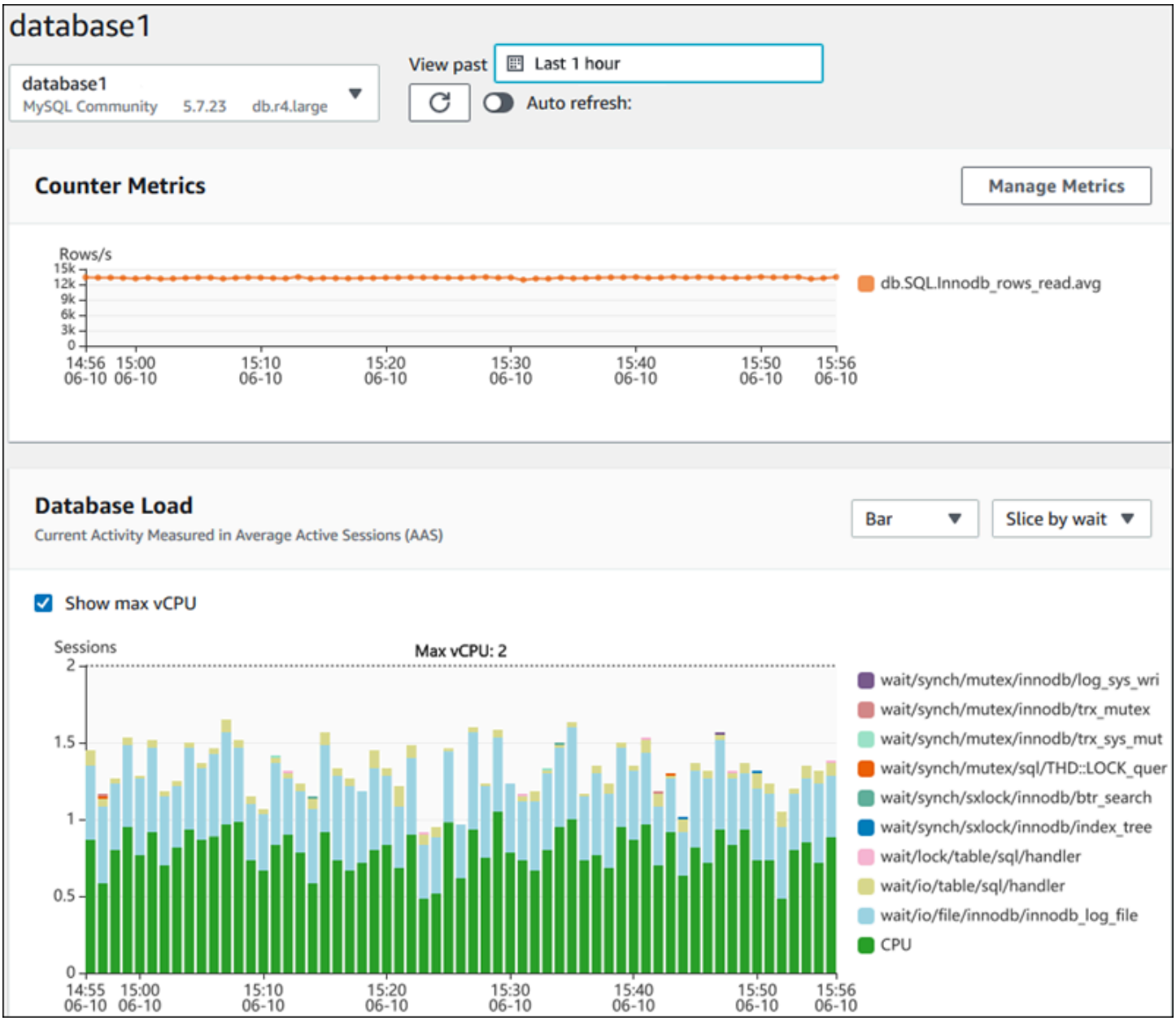


CloudWatch fornisce anche dashboard che puoi utilizzare per creare, personalizzare, interagire e salvare visualizzazioni personalizzate (grafici) delle metriche. È inoltre possibile utilizzare CloudWatch Logs Insights per creare un dashboard per il monitoraggio del registro delle query lente e del registro degli errori e per ricevere avvisi se viene rilevato uno schema specifico in tali registri. La schermata seguente mostra un esempio di dashboard. CloudWatch



Performance Insights di Amazon RDS

Amazon RDS Performance Insights è uno strumento di ottimizzazione e monitoraggio delle prestazioni del database che amplia le funzionalità di monitoraggio di Amazon RDS. Ti aiuta ad analizzare le prestazioni del database visualizzando il carico dell'istanza DB e filtrando il carico per attese, istruzioni SQL, host o utenti. Lo strumento combina più metriche in un unico grafico interattivo che consente di identificare il tipo di collo di bottiglia dell'istanza DB, ad esempio blocchi di attesa, elevato consumo di CPU o latenza di I/O, e determinare quali istruzioni SQL stanno creando il collo di bottiglia. La schermata seguente mostra un esempio di visualizzazione.



Devi abilitare Performance Insights durante il processo di creazione dell'istanza DB per raccogliere i parametri per le istanze DB di Amazon RDS nel tuo account. Il piano gratuito include sette giorni di cronologia dei dati sulle prestazioni e un milione di richieste API al mese. Facoltativamente, puoi acquistare periodi di conservazione più lunghi. Per informazioni sui prezzi, consulta Prezzi di Performance Insights.

Per informazioni su come utilizzare Performance Insights per monitorare le istanze DB, consulta la sezione Monitoraggio delle istanze DB più avanti in questa guida.

Performance Insights pubblica automaticamente le metriche su. CloudWatch Oltre a utilizzare lo strumento Performance Insights, puoi sfruttare le funzionalità aggiuntive che CloudWatch offre. Puoi esaminare le metriche di Performance Insights utilizzando la CloudWatch console AWS CLI, l'o l' CloudWatch API. Puoi anche aggiungere CloudWatch allarmi, come con qualsiasi altra metrica. Ad esempio, potresti voler attivare una notifica SMS ai DBA o intraprendere un'azione correttiva se la `DBLoad` metrica supera il valore di soglia impostato. Puoi anche aggiungere le metriche di Performance Insights ai CloudWatch dashboard esistenti.

Enhanced Monitoring

Enhanced Monitoring è uno strumento che acquisisce i parametri in tempo reale per il sistema operativo (OS) su cui viene eseguita l'istanza database Amazon RDS. Questi parametri forniscono una granularità fino a un secondo per CPU, memoria, processi Amazon RDS e OS, file system e dati di I/O del disco, tra gli altri. Puoi accedere e analizzare questi parametri nella console Amazon RDS. Come per Performance Insights, i parametri di Enhanced Monitoring vengono forniti da Amazon RDS a CloudWatch, dove puoi beneficiare di funzionalità aggiuntive come la conservazione a lungo termine dei parametri per l'analisi, la creazione di filtri per le metriche, la visualizzazione di grafici sulla CloudWatch dashboard e l'impostazione di allarmi. Per impostazione predefinita, Enhanced Monitoring è disabilitato quando crei una nuova istanza database Amazon RDS. Puoi abilitare la funzionalità quando crei o modifichi un'istanza DB. I prezzi si basano sulla quantità di dati trasferiti da Amazon RDS a CloudWatch Logs e sulle tariffe di archiviazione. A seconda della granularità e del numero di istanze DB in cui è abilitato il monitoraggio avanzato, una parte dei dati di monitoraggio può essere inclusa nel piano gratuito di Logs. CloudWatch Per i dettagli completi sui prezzi, consulta la pagina CloudWatch dei prezzi di Amazon. Per ulteriori informazioni sullo strumento, consulta la documentazione di Amazon RDS e le domande frequenti su Enhanced Monitoring.

Servizi aggiuntivi AWS

AWS fornisce diversi servizi di supporto, che si integrano anche con Amazon RDS e CloudWatch per migliorare ulteriormente l'osservabilità dei database. Questi includono Amazon EventBridge, Amazon CloudWatch Logs e AWS CloudTrail.

- Amazon EventBridge è un bus di eventi serverless in grado di ricevere, filtrare, trasformare, indirizzare e distribuire eventi dalle tue applicazioni e AWS risorse, incluse le istanze database Amazon RDS. Un evento Amazon RDS indica una modifica nell'ambiente Amazon RDS. Ad esempio, quando un'istanza DB cambia il suo stato da Available a Stopped, Amazon RDS genera l'evento`RDS-EVENT-0087 / The DB instance has been stopped`. Amazon RDS distribuisce CloudWatch eventi a Events quasi EventBridge in tempo reale. Utilizzando EventBridge and CloudWatch Events, puoi definire regole per inviare avvisi su eventi Amazon RDS specifici di interesse e automatizzare le azioni da intraprendere quando un evento corrisponde alla regola. Sono disponibili diversi obiettivi in risposta a un evento, ad esempio una AWS Lambda funzione in grado di eseguire un'azione correttiva o un argomento di Amazon SNS che può inviare un'e-mail o un SMS per notificare l'evento ai DBA DevOps o ai tecnici.
- Amazon CloudWatch Logs è un servizio che centralizza l'archiviazione dei file di log di tutte le tue applicazioni, sistemi e AWS servizi, tra cui Amazon RDS for MySQL e le istanze database MariaDB e. AWS CloudTrail Se abiliti la funzionalità per le tue istanze DB, Amazon RDS pubblica automaticamente i seguenti log in Logs: CloudWatch
  - Log di errori
  - Log delle query lente
  - Log generale
  - Log di audit

  Puoi utilizzare CloudWatch Logs Insights per interrogare e analizzare i dati di log. La funzionalità include un linguaggio di interrogazione appositamente progettato che consente di cercare eventi di registro che corrispondono ai modelli definiti dall'utente. Ad esempio, puoi tenere traccia del danneggiamento delle tabelle nella tua istanza DB MySQL monitorando il file di registro degli errori per il seguente schema:. `"ERROR 1034 (HY000): Incorrect key file for table '*'; try to repair it OR Table * is marked as crashed"` I dati di registro filtrati possono essere convertiti in metriche. CloudWatch Puoi quindi utilizzare le metriche per creare dashboard con grafici o dati tabulari o impostare un allarme se il valore di soglia definito viene violato. Ciò è particolarmente utile quando si utilizza il registro di controllo, poiché è possibile monitorare, inviare avvisi e intraprendere azioni correttive automaticamente se viene rilevato un comportamento

imprevisto o sospetto. Puoi accedere e gestire i log del database utilizzando la console di AWS gestione AWS CLI, l'API Amazon RDS o l' AWS SDK for Logs. CloudWatch

- AWS CloudTrailregistra e monitora continuamente l'attività degli utenti e delle API nel tuo account AWS. Ti aiuta con il controllo, il monitoraggio della sicurezza e la risoluzione dei problemi operativi delle tue istanze Amazon RDS for MySQL o MariaDB DB. CloudTrail è integrato con Amazon RDS. Tutte le azioni possono essere registrate e CloudTrail fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon RDS. Ad esempio, quando un utente crea una nuova istanza Amazon RDS DB, viene rilevato un evento e il log include informazioni sull'azione richiesta (`"eventName": "CreateDBInstance"`), la data e l'ora dell'azione (`"eventTime": "2022-07-30T22:14:06Z"`), i parametri della richiesta (`"requestParameters": {"dBInstanceIdentifier": "test-instance", "engine": "mysql", "dBInstanceClass": "db.m6g.large"}`) e così via. Gli eventi registrati da CloudTrail includono sia le chiamate dalla console Amazon RDS sia le chiamate dal codice che utilizza l'API Amazon RDS.

Strumenti di monitoraggio di terze parti

In alcuni scenari, oltre alla suite completa di strumenti di monitoraggio e osservabilità nativi del cloud che AWS fornisce Amazon RDS, potresti voler utilizzare strumenti di monitoraggio di altri fornitori di software. Tali scenari includono implementazioni ibride, in cui potresti avere diversi database in esecuzione nel data center locale e un altro set di database in esecuzione nel. Cloud AWS Se hai già creato la tua soluzione di osservabilità aziendale, potresti voler continuare a utilizzare gli strumenti esistenti ed estenderli alle tue distribuzioni nel cloud AWS. La sfida nella configurazione di una soluzione di monitoraggio di terze parti spesso risiede nelle protezioni imposte da Amazon RDS come servizio gestito dal cloud. Ad esempio, non è possibile installare il software agente sul sistema operativo host che esegue l'istanza DB, poiché l'accesso alla macchina host del database è negato. Tuttavia, puoi integrare molte soluzioni di monitoraggio di terze parti con Amazon RDS basandosi su altri Cloud AWS servizi. CloudWatch Ad esempio, i parametri, i log, gli eventi e le tracce di Amazon RDS possono essere esportati e quindi importati nello strumento di monitoraggio di terze parti per ulteriori analisi, visualizzazioni e avvisi. Alcune di queste soluzioni di terze parti includono Prometheus, Grafana e Percona.

Prometheus e Grafana

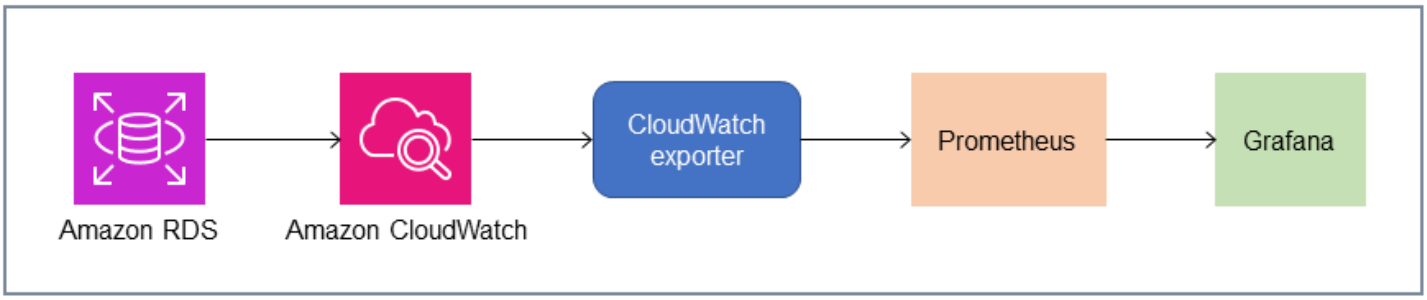
Prometheus è una soluzione di monitoraggio open source che raccoglie metriche da obiettivi configurati a intervalli prestabiliti. È una soluzione di monitoraggio generica in grado di monitorare

qualsiasi applicazione o servizio. Quando monitori le istanze DB di Amazon RDS, CloudWatch raccoglie i parametri da Amazon RDS. Le metriche vengono quindi esportate sul server Prometheus utilizzando un esportatore open source come YACE exporter o Exporter. CloudWatch

- L'esportatore YACE ottimizza le attività di esportazione dei dati recuperando diverse metriche in un'unica richiesta all'API. CloudWatch Dopo che le metriche sono state archiviate sul server Prometheus, il server valuta le espressioni delle regole e può generare avvisi quando vengono rispettate le condizioni specificate.
- CloudWatch Exporter è ufficialmente gestito da Prometheus. Recupera le CloudWatch metriche tramite l' CloudWatch API e le archivia sul server Prometheus in un formato compatibile con Prometheus, utilizzando le richieste API REST all'endpoint HTTP.

Quando scegli un esportatore, progetti il tuo modello di implementazione e configuri le istanze di esportazione, prendi in considerazione CloudWatche CloudWatch registra le quote del servizio e delle API, poiché l'esportazione delle metriche CloudWatch su un server Prometheus è implementata sull'API. CloudWatch Ad esempio, l'implementazione di più istanze di CloudWatch Exporter in un'unica regione per monitorare centinaia di istanze DB di Amazon RDS potrebbe causare un errore di throttling () Account AWS e un codice di 400 errori. ThrottlingException Per superare tali limitazioni, prendi in considerazione l'utilizzo di YACE exporter, che è ottimizzato per raccogliere fino a 500 parametri diversi in una singola richiesta. Inoltre, per distribuire un gran numero di istanze database Amazon RDS, dovresti prendere in considerazione l'utilizzo di più istanze Account AWS, anziché centralizzare il carico di lavoro in un'unica Account AWS istanza e limitare il numero di istanze di esportazione in ciascuna. Account AWS

Gli avvisi vengono generati dal server Prometheus e gestiti da Alertmanager. Questo strumento si occupa di deduplicare, raggruppare e indirizzare gli avvisi al destinatario corretto, ad esempio e-mail, SMS o Slack, o di avviare un'azione di risposta automatica. Un altro strumento open source chiamato Grafana mostra le visualizzazioni per queste metriche. Grafana offre ricchi widget di visualizzazione, come grafici avanzati, dashboard dinamici e funzionalità di analisi come query ad hoc e drilldown dinamico. Può anche cercare e analizzare i log e include funzionalità di avviso per valutare continuamente metriche e log e inviare notifiche quando i dati soddisfano le regole di avviso.



Percona

Percona Monitoring and Management (PMM) è una soluzione gratuita e open source di monitoraggio, gestione e osservabilità di database per MySQL e MariaDB. PMM raccoglie migliaia di metriche prestazionali dalle istanze DB e dai relativi host. Fornisce un'interfaccia utente Web per visualizzare i dati nei dashboard e funzionalità aggiuntive come consulenti automatici per le valutazioni dello stato del database. Puoi usare PMM per monitorare Amazon RDS. Tuttavia, il client PMM (agente) non è installato sugli host sottostanti delle istanze DB di Amazon RDS, perché non ha accesso agli host. Lo strumento si connette invece alle istanze DB di Amazon RDS, interroga le statistiche del server`INFORMATION_SCHEMA`, lo schema di sistema e lo schema delle prestazioni e utilizza l' CloudWatch API per acquisire metriche, log, eventi e tracce. PMM richiede una chiave di accesso utente AWS Identity and Access Management (IAM) (ruolo IAM) e rileva automaticamente le istanze DB di Amazon RDS disponibili per il monitoraggio. Lo strumento PMM è profilato per il monitoraggio del database e raccoglie più metriche specifiche del database rispetto a Prometheus. Per utilizzare la dashboard di PMM Query Analytics, devi configurare lo schema delle prestazioni come origine delle query, poiché l'agente Query Analytics non è installato per Amazon RDS e non può leggere il log delle query lente. Invece, interroga `performance_schema` direttamente le istanze DB MySQL e MariaDB per ottenere le metriche. Una delle caratteristiche principali di PMM è la sua capacità di avvisare e consigliare i DBA sui problemi che lo strumento identifica nei loro database. PMM offre una serie di controlli in grado di rilevare le minacce alla sicurezza più comuni, il degrado delle prestazioni, la perdita e il danneggiamento dei dati.

Oltre a questi strumenti, sul mercato sono disponibili diverse soluzioni commerciali di osservabilità e monitoraggio che possono integrarsi con Amazon RDS. Gli esempi includono Datadog Database Monitoring, Dynatrace Amazon RDS Monitoring e Database Monitoring. AppDynamics

Monitoraggio delle istanze database

UNIstanza DBè l'elemento costitutivo di base di Amazon RDS. È un ambiente di database isolato che viene eseguito nel cloud. Per i database MySQL e MariaDB, l'istanza DB èmysqldprogramma, noto anche come server MySQL, che include più thread e componenti come il parser SQL, l'ottimizzatore di query, il gestore di thread/connessioni, variabili di sistema e di stato e uno o più motori di archiviazione collegabili. Ogni motore di storage è progettato per supportare un caso d'uso specializzato. Il motore di archiviazione predefinito e consigliato èInnoDB, che è un motore di database relazionale transazionale, generico e conforme al modello ACID (atomicity, consistency, isolation, durability). Funzionalità di InnoDBstrutture in memoria(buffer pool, change buffer, adaptive hash index, log buffer) estrutture su disco(tablespace, tabelle, indici, registro di annullamento, redo log, file buffer di doppia scrittura). Per garantire che il database aderisca strettamente al modello ACID,Il motore di storage InnoDB implementa numerose funzionalitàper proteggere i tuoi dati, tra cui transazioni, commit, rollback, crash recovery, blocco a livello di riga e controllo della concorrenza multiversione (MVCC).

Tutti questi componenti interni di un'istanza database funzionano congiuntamente per contribuire a mantenere la disponibilità, l'integrità e la sicurezza dei dati al livello di prestazioni previsto e soddisfacente. A seconda del carico di lavoro, ogni componente e funzionalità potrebbero richiedere risorse a CPU, memoria, rete e sottosistemi di storage. Quando un aumento della domanda di una risorsa specifica supera la capacità fornita o i limiti software per quella risorsa (imposti dai parametri di configurazione o dalla progettazione del software), l'istanza database può subire un degrado delle prestazioni o una completa indisponibilità e danneggiamento. Pertanto, è fondamentale misurare e monitorare questi componenti interni, confrontarli con i valori di base definiti e generare avvisi se i valori monitorati si discostano dai valori previsti.

Come descritto in precedenza, puoi usare diversiutensiliper monitorare le tue istanze MySQL e MariaDB. Ti consigliamo di utilizzare Amazon RDS Performance Insights eCloudWatchstrumenti per il monitoraggio e la segnalazione, poiché questi strumenti sono integrati con Amazon RDS, raccolgono metriche ad alta risoluzione, presentano le informazioni più recenti sulle prestazioni quasi in tempo reale e generano allarmi.

Indipendentemente dal tuo strumento di monitoraggio preferito, ti consigliamo diattivare lo schema delle prestazioninelle tue istanze DB MySQL e MariaDB. LaSchema delle prestazioniè una funzionalità opzionale per il monitoraggio del funzionamento del server MySQL (l'istanza DB) a basso livello ed è progettata per avere un impatto minimo sulle prestazioni complessive del database. È possibile gestire questa funzionalità utilizzando`performance_schema`parametro. Sebbene

questo parametro sia facoltativo, devi utilizzarlo per raccogliere metriche per SQL ad alta risoluzione (un secondo), metriche delle sessioni attive, eventi di attesa e altre informazioni di monitoraggio dettagliate e di basso livello, raccolte da Amazon RDS Performance Insights.

Sezioni

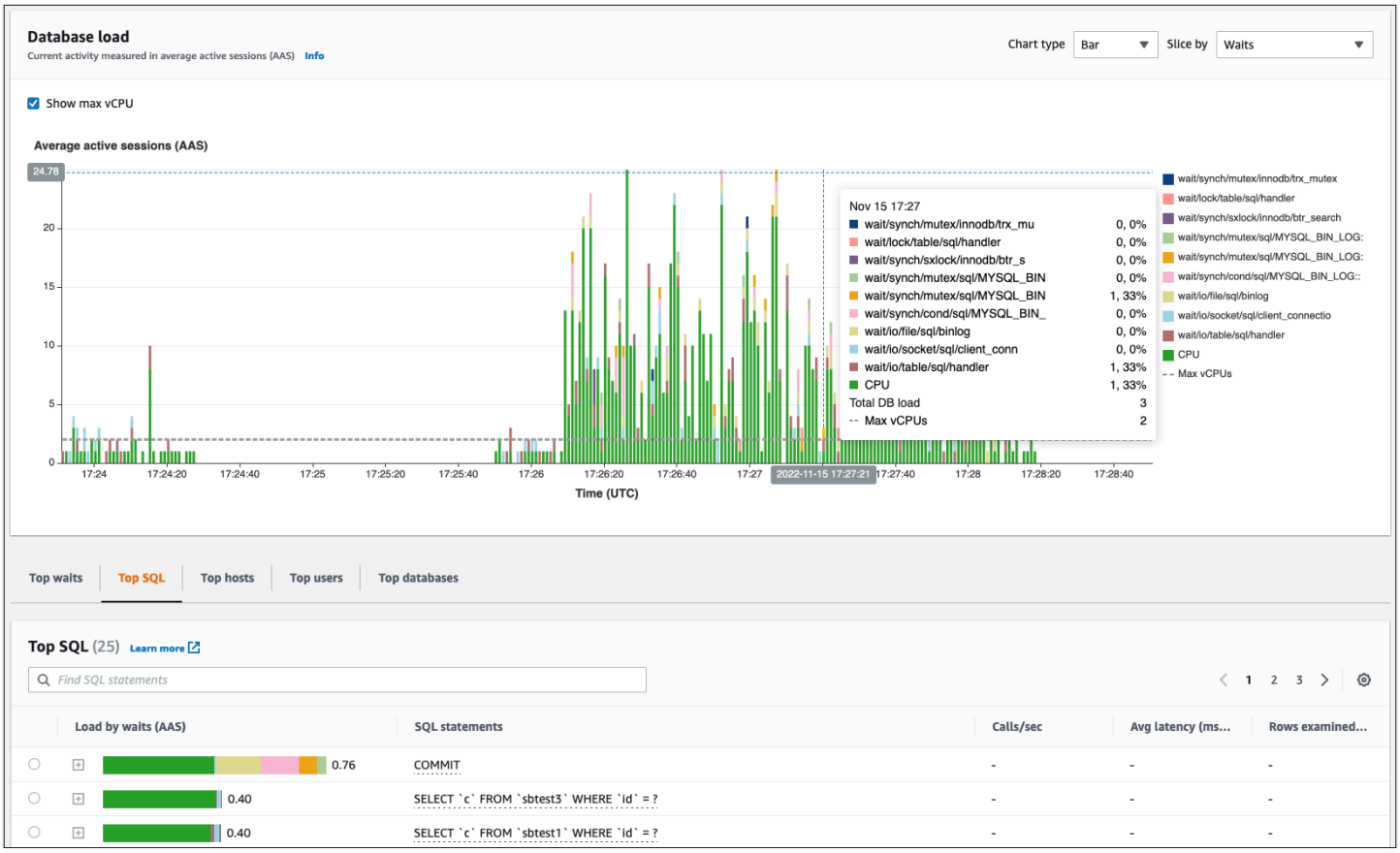
Metriche di Performance Insights per le istanze DB

Performance Insights monitora diversi tipi di metriche, come discusso nelle sezioni seguenti.

Caricamento database

Caricamento del database (`DBLoad`) è una metrica chiave di Performance Insights che misura il livello di attività nel tuo database. Viene raccolto ogni secondo e pubblicato automaticamente su AmazonCloudWatch. Rappresenta l'attività dell'istanza database in sessioni attive medie (AAS), ovvero il numero di sessioni che eseguono contemporaneamente query SQL. La`DBLoad`la metrica è diversa dalle altre metriche delle serie temporali, perché può essere interpretata utilizzando una di queste cinque dimensioni: attese, SQL, host, utenti e database. Queste dimensioni sono sottocategorie di`DBLoad`metrico. Puoi usarli comefetta percategorie per rappresentare le diverse caratteristiche del carico del database. Per una descrizione dettagliata di come calcoliamo il carico del database, vedereCaricamento del databasenella documentazione di Amazon RDS.

La seguente illustrazione della schermata mostra lo strumento Performance Insights.



Dimensioni

- Attendere gli eventisono condizioni in cui una sessione del database attende il completamento di una risorsa o di un'altra operazione per continuare l'elaborazione. Se si esegue un'istruzione SQL come`SELECT * FROM big_table`e se questa tabella è molto più grande del pool di buffer InnoDB allocato, molto probabilmente la tua sessione aspetterà`wait/io/file/innodb/innodb_data_file`eventi di attesa, causati da operazioni fisiche di I/O sul file di dati. Gli eventi di attesa sono una dimensione importante per il monitoraggio del database, poiché indicano possibili rallentamenti delle prestazioni. Gli eventi di attesa indicano le risorse e le operazioni che le istruzioni SQL eseguite all'interno delle sessioni impiegano più tempo ad aspettare. Ad esempio,`wait/synch/mutex/innodb/trx_sys_mutex`l'evento si verifica quando c'è un'elevata attività del database con un numero elevato di transazioni e`wait/synch/mutex/innodb/buf_pool_mutex`l'evento si verifica quando un thread ha acquisito un blocco sul pool di buffer di InnoDB per accedere a una pagina in memoria. Per informazioni su tutti gli eventi di attesa di MySQL e MariaDB, vedereTabelle di riepilogo degli eventi di attesanella documentazione di MySQL. Per capire come interpretare i nomi degli strumenti, vedereConvenzioni di denominazione degli strumenti dello schema delle prestazioninella documentazione di MySQL.

- SQLmostra quali istruzioni SQL contribuiscono maggiormente al carico totale del database. LaDimensioni superioritavolo, che si trova sotto ilCaricamento del databaseil grafico in Amazon RDS Performance Insights è interattivo. È possibile ottenere un elenco dettagliato degli eventi di attesa associati all'istruzione SQL facendo clic sulla barra nelCaricamento in attesa (AAS)colonna. Quando si seleziona un'istruzione SQL nell'elenco, Performance Insights visualizza gli eventi di attesa associati nelCaricamento del databasegrafico e il testo dell'istruzione SQL neltesto SQLsezione. Le statistiche SQL vengono visualizzate sul lato destro delDimensioni superioritavolo.
- Padronimostra i nomi degli host dei client connessi. Questa dimensione consente di identificare quali host client inviano la maggior parte del carico al database.
- Utentiraggruppa il carico del DB da parte degli utenti che hanno effettuato l'accesso al database.
- Banche datiraggruppa il carico del database in base al nome del database a cui è connesso il client.

Parametri dei contatori

Le contatori sono metriche cumulative i cui valori possono aumentare o azzerarsi solo al riavvio dell'istanza database. Il valore di una contometrica non può essere ridotto al valore precedente. Queste metriche rappresentano un singolo contatore che aumenta in modo monotono.

- Contatori nativisono metriche definite dal motore del database e non da Amazon RDS. Ad esempio:
  - `SQL.Innodb_rows_inserted`rappresenta il numero di righe inserite nelle tabelle InnoDB.
  - `SQL.Select_scan`rappresenta il numero di join che hanno completato una scansione completa della prima tabella.
  - `Cache.Innodb_buffer_pool_reads`rappresenta il numero di letture logiche che il motore InnoDB non è riuscito a recuperare dal pool di buffer e ha dovuto leggere direttamente dal disco.
  - `Cache.Innodb_buffer_pool_read_requests`rappresenta il numero di richieste di lettura logiche.

  Per le definizioni di tutte le metriche native, vediVariabili di stato del servernella documentazione di MySQL.
- Contatori non nativisono definiti da Amazon RDS. Puoi ottenere queste metriche utilizzando una query specifica o derivarle utilizzando due o più metriche native nei calcoli. Le metriche dei contatori non native possono rappresentare latenze, rapporti o percentuali di successo. Ad esempio:

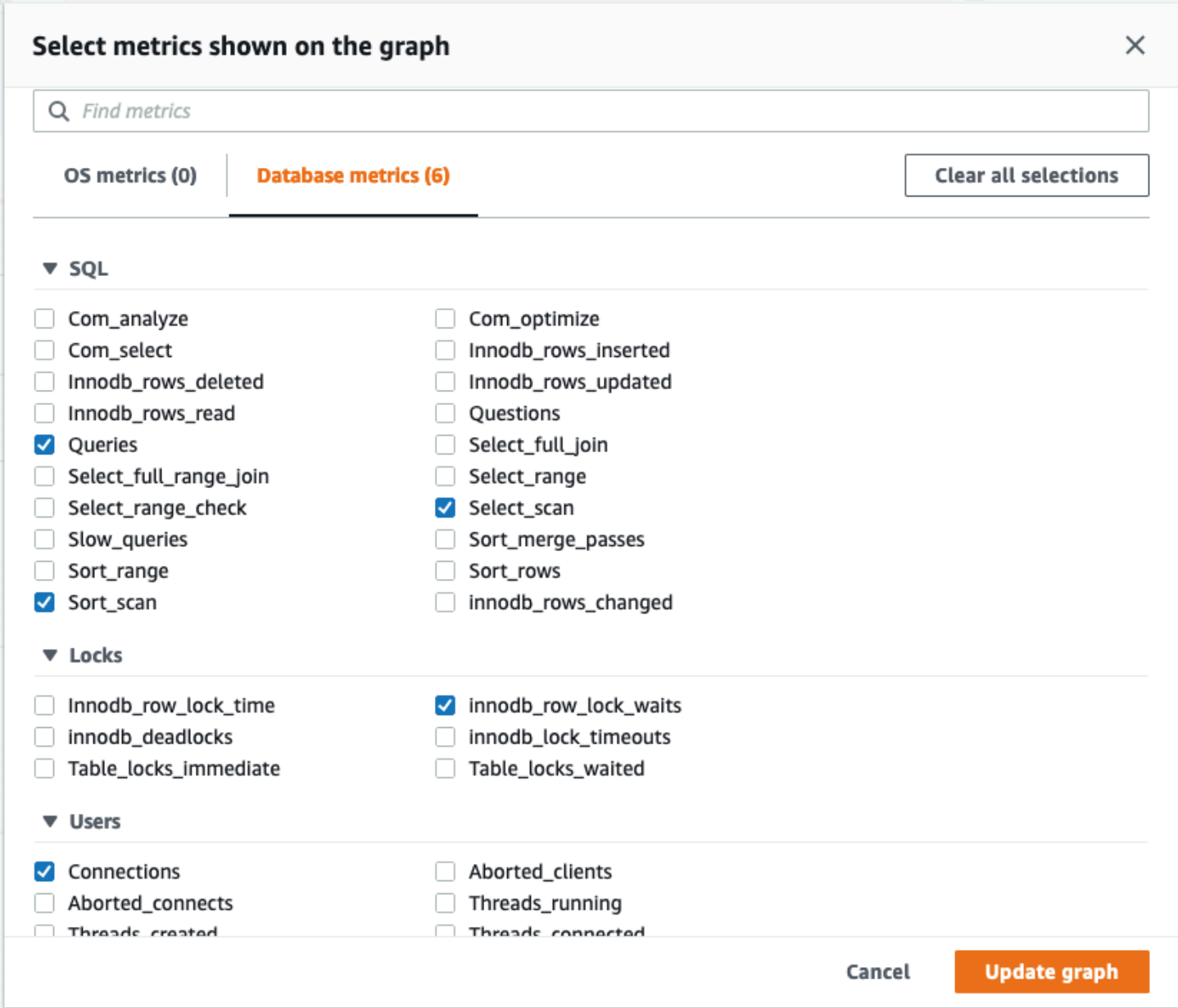
- `Cache.innoDB_buffer_pool_hits`rappresenta il numero di operazioni di lettura che InnoDB può recuperare dal pool di buffer senza utilizzare il disco. Viene calcolato in base alle metriche dei contatori nativi come segue:

  ```
  db.Cache.Innodb_buffer_pool_read_requests - db.Cache.Innodb_buffer_pool_reads
  ```

- `IO.innoDB_datafile_writes_to_disk`rappresenta il numero di operazioni di scrittura di file di dati InnoDB su disco. Cattura solo le operazioni sui file di dati, non le operazioni di doppia scrittura o redo logging e scrittura. Viene calcolato come segue:

  ```
  db.IO.Innodb_data_writes - db.IO.Innodb_log_writes - db.IO.Innodb_dblwr_writes
  ```

Puoi visualizzare le metriche delle istanze DB direttamente nella dashboard di Performance Insights. ScegliGestisci le metriche, scegli laMetriche del databaseTocca, quindi seleziona le metriche di interesse, come mostrato nella figura seguente.



Scegli laAggiorna graficopulsante per visualizzare le metriche selezionate, come mostrato nella figura seguente.

Statistiche SQL

Performance Insights raccoglie metriche relative alle prestazioni sulle query SQL per ogni secondo di esecuzione di una query e per ogni chiamata SQL. In generale, Performance Insights raccoglieStatistiche SQLa livello di dichiarazione e riassunto. Tuttavia, per le istanze DB di MariaDB e MySQL, le statistiche vengono raccolte solo a livello di riepilogo.

- Digest statistics è una metrica composita di tutte le query che hanno lo stesso schema ma che alla fine hanno valori letterali diversi. Il digest sostituisce valori letterali specifici con una variabile; ad esempio:

```
SELECT department_id, department_name FROM departments WHERE location_id = ?
```

- Esistono metriche che rappresentano le statisticheal secondoper ogni istruzione SQL digerita. Ad esempio,`sql_tokenized.stats.count_star_per_sec`rappresenta le chiamate al secondo (ovvero, quante volte al secondo è stata eseguita l'istruzione SQL).

- Performance Insights include anche metriche che fornisconoper chiamatastatistiche per un'istruzione SQL. Ad esempio,`sql_tokenized.stats.sum_timer_wait_per_call`mostra la latenza media dell'istruzione SQL per chiamata, in millisecondi.

Le statistiche SQL sono disponibili nella dashboard di Performance Insights, nell migliori SQLscheda delDimensioni superioritavolo.

CloudWatchmetriche per le istanze DB

AmazonCloudWatchcontiene anche metriche che Amazon RDS pubblica automaticamente. Le metriche che risiedono nel`AWS/RDS`i namespace sonometriche a livello di istanza, che si riferisce all'istanza Amazon RDS (servizio) (ovvero all'ambiente di database isolato in esecuzione nel cloud) anziché all'istanza database in senso strettomysqldprocesso. Pertanto, la maggior parte di questimetriche predefiniterientrano nella categoria delle metriche del sistema operativo, nella definizione rigorosa del termine. Gli esempi includono:`CPUUtilization`,`WriteIOPS`,`SwapUsage`e altri ancora. Tuttavia, ci sono alcune metriche delle istanze DB applicabili a MariaDB e MySQL:

- `BinLogDiskUsage`— La quantità di spazio su disco occupata dai log binari.
- `DatabaseConnections`— Il numero di connessioni di rete client all'istanza database.
- `ReplicaLag`— La quantità di tempo in cui un'istanza database di replica di lettura è in ritardo rispetto all'istanza database di origine.

Pubblicazione delle metriche di Performance Insights suCloudWatch

Amazon RDS Performance Insights monitora la maggior parte delle metriche e delle dimensioni delle istanze database e le rende disponibili tramite la dashboard di Performance Insights nelAWSConsole

di gestione. Questa dashboard è ideale per la risoluzione dei problemi dei database e l'analisi delle cause principali. Tuttavia, non è possibile creare allarmi in Performance Insights per le metriche relative alle prestazioni. Per creare allarmi basati sulle metriche di Performance Insights, devi spostare tali metriche suCloudWatch. Avere le metriche inCloudWatchti dà anche accesso a funzionalità di monitoraggio avanzate comeCloudWatchrilevamento delle anomalie,matematica metrica, estatistichee puoi esportare le metriche su strumenti di monitoraggio esterni come Prometheus e Grafana.

Le metriche di Performance Insights non vengono pubblicate automaticamente suCloudWatch(ad eccezione delmetrica DB Load). Per pubblicare le metriche delle istanze DB da Performance Insights suCloudWatch, puoi usare ilAPI Performance Insightsper recuperare le metriche eCloudWatchAPIper pubblicare metriche suCloudWatch. Per automatizzare il processo, puoi creare una funzione Lambda e pianificarla in AmazonEventBridgeda eseguire in periodi di tempo specificati, ad esempio ogni due minuti. Puoi specificare su quali metriche di Performance Insights desideri pubblicareCloudWatch. La funzione Lambda ottiene le metriche da tutte le istanze di Amazon RDS con Performance Insights abilitato e le salva inCloudWatch. Per ulteriori informazioni su questo processo, consulta il post sul blog sufornitura delle metriche dei contatori di Performance Insights aCloudWatch.

monitoraggio del sistema operativo

Un'istanza database in Amazon RDS per MySQL o MariaDB viene eseguita sul sistema operativo Linux, che utilizza le risorse di sistema sottostanti: CPU, memoria, rete e storage.

```
MySQL [(none)]> SHOW variables LIKE 'version%';
+-------------------------+---------------------+
| Variable_name           | Value               |
+-------------------------+---------------------+
| version                 | 8.0.28              |
| version_comment         | Source distribution |
| version_compile_machine | aarch64             |
| version_compile_os      | Linux               |
| version_compile_zlib    | 1.2.11              |
+-------------------------+---------------------+
5 rows in set (0.00 sec)
```

Le prestazioni complessive del database e del sistema operativo sottostante dipendono fortemente dall'utilizzo delle risorse di sistema. Ad esempio, la CPU è il componente chiave per le prestazioni del sistema, poiché esegue le istruzioni del software del database e gestisce altre risorse di sistema. Se la CPU è sovrautilizzata (ovvero, se il carico richiede più potenza della CPU rispetto a quella fornita per l'istanza database), questo problema influirebbe sulle prestazioni e sulla stabilità del database e, di conseguenza, dell'applicazione.

Il motore del database alloca e libera la memoria in modo dinamico. Quando la memoria RAM non è sufficiente per eseguire il lavoro corrente, il sistema scrive pagine di memoria nella memoria di swap, che risiede sul disco. Poiché il disco è molto più lento della memoria, anche se è basato sulla tecnologia SSD NVMe, un'allocazione eccessiva di memoria porta a un peggioramento delle prestazioni. L'elevato utilizzo della memoria causa una maggiore latenza delle risposte del database, poiché la dimensione di un file di pagina aumenta per supportare memoria aggiuntiva. Se l'allocazione di memoria è così elevata da esaurire sia la RAM che gli spazi di memoria di swap, il servizio di database potrebbe non essere disponibile e gli utenti potrebbero riscontrare errori come`[ERROR] mysqld: Out of memory (Needed xyz bytes)`.

I sistemi di gestione dei database MySQL e MariaDB utilizzano il sottosistema di archiviazione, che è costituito da dischi che memorizzanostrutture su discoad esempio tabelle, indici, log binari, redo log, undo log e file buffer di doppia scrittura. Pertanto, il database, a differenza di altri tipi di software, deve eseguire molte attività su disco. Per un funzionamento ottimale del database, è

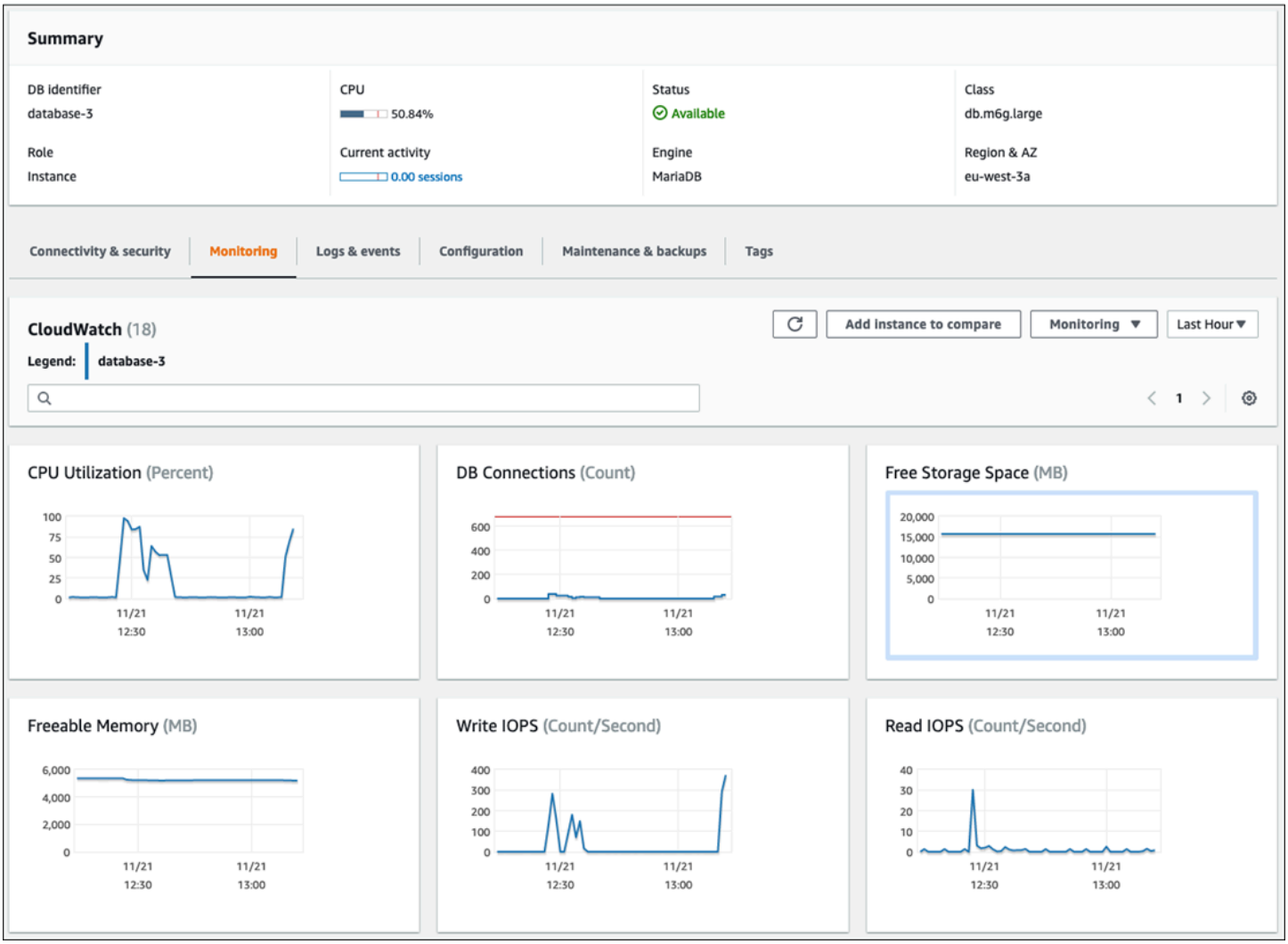
importante monitorare e ottimizzare l'utilizzo degli I/O del disco e l'allocazione dello spazio su disco. Le prestazioni del database possono essere influenzate quando il database raggiunge i limiti massimi di IOPS o di throughput supportati dal disco. Ad esempio, le interruzioni di accesso casuali causate da una scansione dell'indice possono causare un numero elevato di operazioni di I/O al secondo, con conseguenti limitazioni dello storage sottostante. Le scansioni complete della tabella potrebbero non raggiungere il limite IOPS, ma potrebbero causare una velocità effettiva elevata misurata in megabyte al secondo. È fondamentale monitorare e generare avvisi sull'allocazione dello spazio su disco, poiché errori come`OS error code 28: No space left on device`può causare l'indisponibilità e il danneggiamento del database.

Amazon RDS fornisce metriche in tempo reale per il sistema operativo su cui viene eseguita l'istanza database. Amazon RDS pubblica automaticamente un set di parametri del sistema operativo suCloudWatch. Queste metriche sono disponibili per la visualizzazione e l'analisi nella console Amazon RDS e nelCloudWatchdashboard e puoi impostare allarmi sulle metriche selezionate inCloudWatch. Esempi includono:

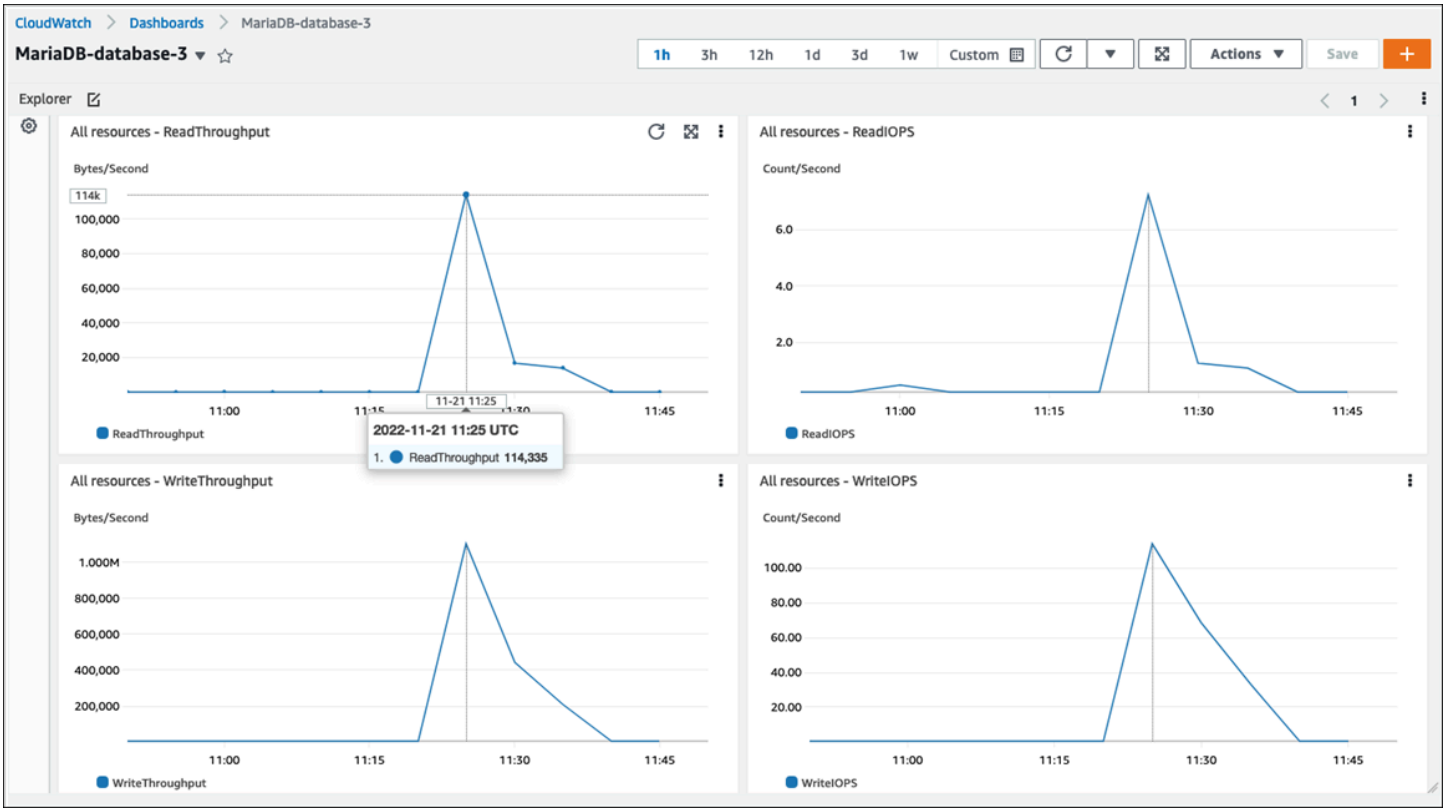
- `CPUUtilization`— La percentuale di utilizzo della CPU.
- `BinLogDiskUsage`— La quantità di spazio su disco occupata dai log binari.
- `FreeableMemory`— La quantità di memoria ad accesso casuale disponibile. Questo rappresenta il valore del`MemAvailable`campo di`/proc/meminfo`.
- `ReadIOPS`— Il numero medio di operazioni I/O di lettura su disco al secondo.
- `WriteThroughput`— Il numero medio di byte scritti su disco al secondo per l'archiviazione locale.
- `NetworkTransmitThroughput`— Il traffico di rete in uscita sul nodo DB, che combina il traffico del database e il traffico Amazon RDS utilizzato per il monitoraggio e la replica.

Per un riferimento completo di tutte le metriche pubblicate da Amazon RDS aCloudWatch, vediAmazonCloudWatchmetriche per Amazon RDSnella documentazione di Amazon RDS.

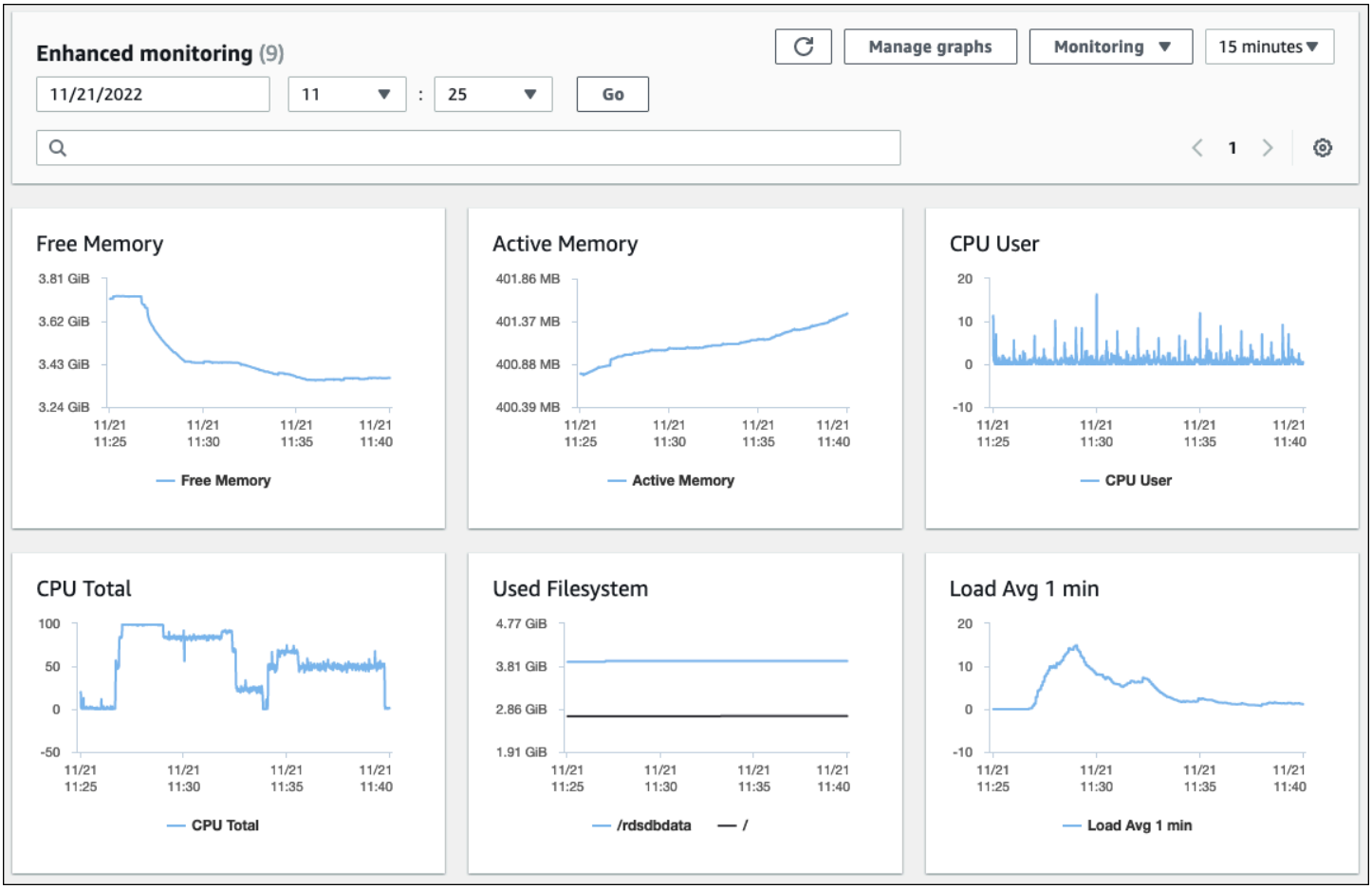
La tabella seguente mostra esempi diCloudWatchmetriche per Amazon RDS visualizzate sulla console Amazon RDS.



Il grafico seguente mostra metriche simili visualizzate nelCloudWatchcruscotto.



L'altro set di metriche del sistema operativo viene raccolto daMonitoraggio miglioratoper Amazon RDS. Questo strumento ti offre una visibilità più approfondita sullo stato delle tue istanze database Amazon RDS for MariaDB e Amazon RDS for MySQL, fornendo metriche di sistema e informazioni sui processi del sistema operativo in tempo reale. Quando tuabilitare il monitoraggio avanzatosull'istanza DB e imposta la granularità desiderata, lo strumento raccoglie le metriche del sistema operativo e le informazioni sul processo, che è possibile visualizzare e analizzare sulConsole Amazon RDS, come mostrato nella schermata seguente.



Alcune delle metriche chiave fornite da Enhanced Monitoring sono:

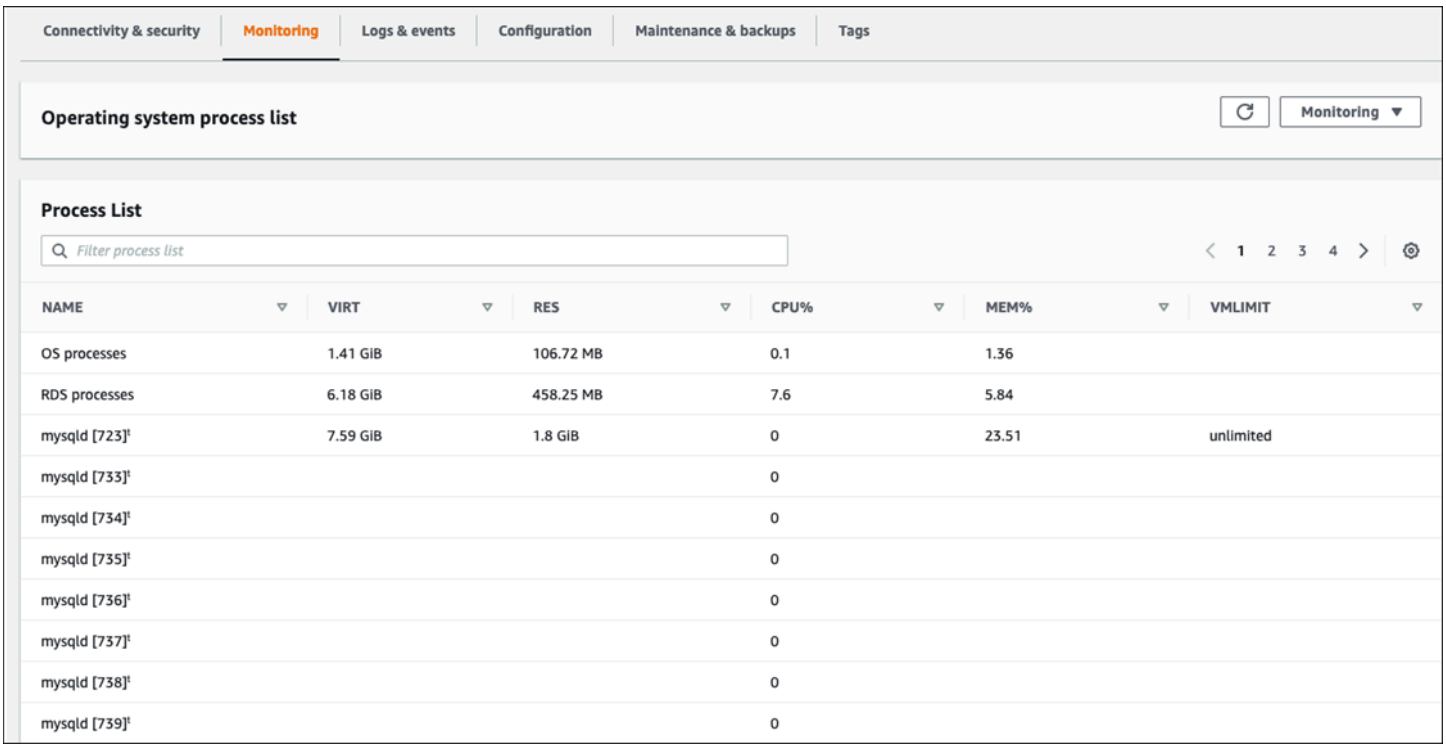
- `cpuUtilization.total`— La percentuale totale della CPU in uso.
- `cpuUtilization.user`— La percentuale di CPU utilizzata dai programmi utente.
- `memory.active`— La quantità di memoria assegnata, in kilobyte.
- `memory.cached`— La quantità di memoria utilizzata per la memorizzazione nella cache degli I/O basati sul file system.
- `loadAverageMinute.one`— Il numero di processi che hanno richiesto il tempo della CPU durante l'ultimo minuto.

Per un elenco completo delle metriche, consultaMetriche del sistema operativo nel monitoraggio avanzatonella documentazione di Amazon RDS.

Sulla console Amazon RDS, l'elenco dei processi del sistema operativo fornisce i dettagli di ogni processo in esecuzione nella tua istanza database. L'elenco è organizzato in tre sezioni:

- Processi del sistema operativo– Questa sezione rappresenta un riepilogo aggregato di tutti i processi del kernel e del sistema. Questi processi hanno generalmente un impatto minimo sulle prestazioni del database.
- Processi RDS— Questa sezione rappresenta un riepilogo delAWSprocessi necessari per supportare un'istanza database Amazon RDS. Ad esempio, include l'agente di gestione di Amazon RDS, i processi di monitoraggio e diagnostica e processi simili.
- Processi secondari RDS— Questa sezione rappresenta un riepilogo dei processi Amazon RDS che supportano l'istanza database, in questo caso`mysqld`processo e relativi thread. La`mysqld`di thread appaiono annidati sotto il genitore`mysqld`processo.

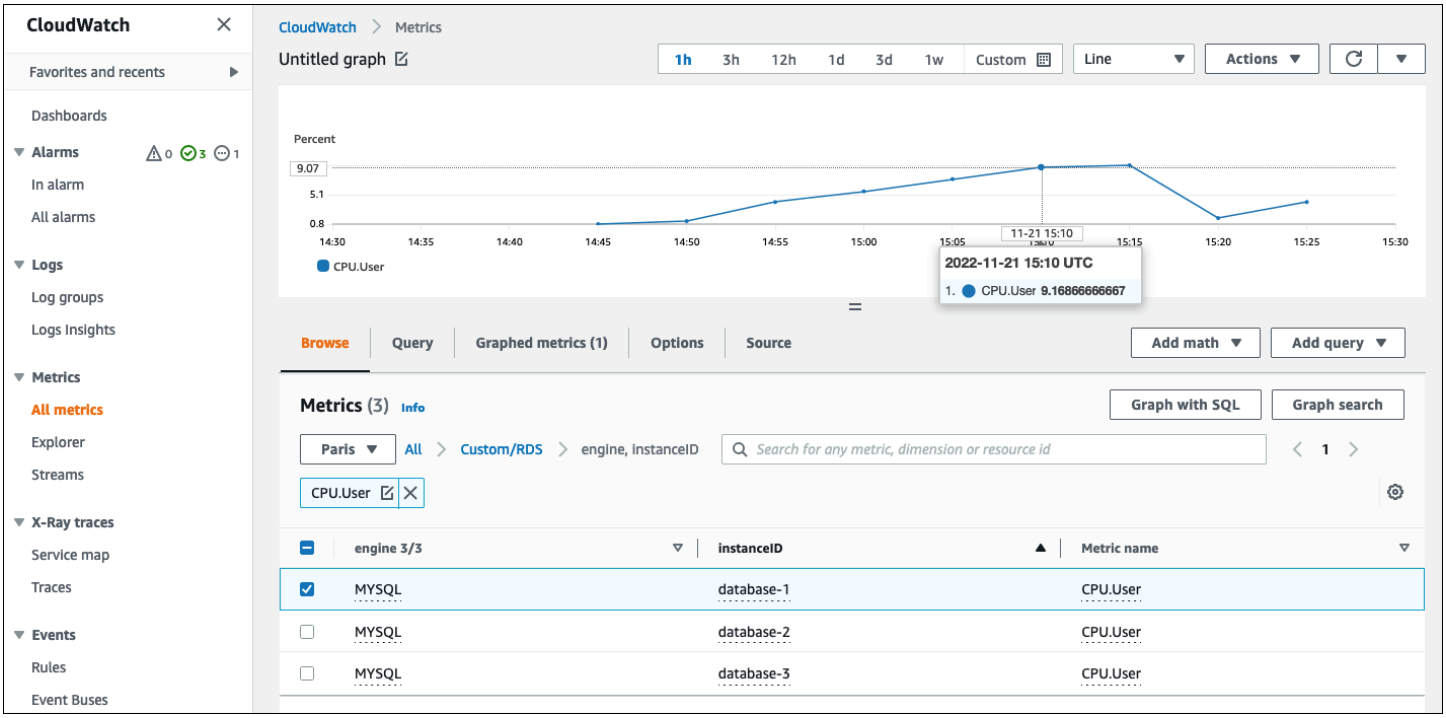
La seguente illustrazione della schermata mostra l'elenco dei processi del sistema operativo nella console Amazon RDS.



Amazon RDS fornisce le metriche di Enhanced Monitoring nel tuoCloudWatchRegistra l'account. I dati di monitoraggio visualizzati sulla console Amazon RDS vengono recuperati daCloudWatchTronchi. Puoi anche[recupera le metriche per un'istanza DB come flusso di log](#)daCloudWatchTronchi. Queste metriche sono archiviate in formato JSON. È possibile utilizzare l'output JSON di Enhanced Monitoring daCloudWatchAccedi a un sistema di monitoraggio di tua scelta.

Per visualizzare i grafici sulCloudWatchdashboard e crea allarmi che avviano un'azione se una metrica supera la soglia definita, devi creare filtri metrici inCloudWatchdaCloudWatchTronchi. Per istruzioni dettagliate, consulta laArticolo su AWS Re:POSTsu come filtrare Enhanced MonitoringCloudWatchRegistri per generare metriche personalizzate automatizzate per Amazon RDS.

L'esempio seguente illustra la metrica personalizzata`CPU.User`nel`Custom/RDS`namespace. Questa metrica personalizzata viene creata filtrando il`cpuUtilization.user`Metrica di monitoraggio migliorata daCloudWatchTronchi.



Quando la metrica è disponibile nelCloudWatcharchivio, puoi visualizzarlo e analizzarlo inCloudWatchdashboard, applica ulteriori operazioni matematiche e di interrogazione e imposta un allarme per monitorare questa metrica specifica e generare avvisi se i valori osservati non sono in linea con le condizioni di allarme definite.

Eventi, registri e percorsi di controllo

MonitoraggioMetriche delle istanze DBeMetriche del sistema operativo, l'analisi delle tendenze e il confronto delle metriche con i valori di base e la generazione di avvisi quando i valori superano le soglie definite sono tutte procedure necessarie e ottimali per aiutarti a raggiungere e mantenere l'affidabilità, la disponibilità, le prestazioni e la sicurezza delle tue istanze database Amazon RDS. Tuttavia, una soluzione completa deve anche monitorare gli eventi del database, i file di registro e gli audit trail dei database MySQL e MariaDB.

Sezioni

Eventi Amazon RDS

UnAmazon Evento RDSindica una modifica nell'ambiente Amazon RDS. Ad esempio, quando lo stato dell'istanza database cambia daAvvioaDisponibile, Amazon RDS genera l'evento`RDS-EVENT-0088` `The DB instance has been started`. Amazon RDS offre eventi ad AmazonEventBridgequasi in tempo reale. Puoi accedere agli eventi tramite la console Amazon RDS,AWS CLIcomandodescrivi gli eventio il funzionamento dell'API Amazon RDSDescribeEvents. La seguente illustrazione della schermata mostra gli eventi e i log visualizzati sulla console Amazon RDS.

Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

CloudWatch alarms (3)

Edit alarm | Create alarm

Filter by alarms

1

Name	State	More options
ApplicationInsights/RDS-DBS/AWS/RDS/CPUUtilization/database-1/	OK	view
ApplicationInsights/RDS-DBS/AWS/RDS/ReadLatency/database-1/	OK	view
ApplicationInsights/RDS-DBS/AWS/RDS/WriteLatency/database-1/	OK	view

Recent events (9)

Filter by db events

1 2

Time	System notes
November 28, 2022, 14:31 (UTC+01:00)	Backing up DB instance
November 28, 2022, 14:32 (UTC+01:00)	Finished DB Instance backup
November 28, 2022, 16:30 (UTC+01:00)	Applying modification to database instance class
November 28, 2022, 16:32 (UTC+01:00)	DB instance shutdown
November 28, 2022, 16:35 (UTC+01:00)	DB instance restarted

Logs (14)

View | Watch | Download

Filter by db logs

1 2 3

Name	Last written	Logs
error/mysql-error-running.log	November 28, 2022, 17:00 (UTC+01:00)	0 bytes
error/mysql-error-running.log.2022-11-28.16	November 28, 2022, 16:40 (UTC+01:00)	3.3 kB
error/mysql-error.log	November 29, 2022, 11:20 (UTC+01:00)	0 bytes
mysqlUpgrade	October 10, 2022, 17:05 (UTC+02:00)	1 kB

Amazon RDS emette diversi tipi di eventi, tra cui eventi di istanze database, eventi di gruppi di parametri DB, eventi di gruppi di sicurezza del database, eventi snapshot del database, eventi proxy RDS ed eventi di distribuzione blu/verdi. Le informazioni includono:

- Nome e tipo di fonte; ad esempio:`"SourceIdentifier": "database-1", "SourceType": "db-instance"`
- Data e ora dell'evento, ad esempio:`"Date": "2022-12-01T09:20:28.595000+00:00"`
- Messaggio associato all'evento, ad esempio:`"Message": "Finished updating DB parameter group"`
- Categoria di evento; ad esempio:`"EventCategories": ["configuration change"]`

Per un riferimento completo, vedereCategorie di eventi e messaggi di eventi Amazon RDSnella documentazione di Amazon RDS.

Ti consigliamo di monitorare gli eventi di Amazon RDS, poiché questi eventi indicano cambiamenti di stato nella disponibilità delle istanze database, modifiche alla configurazione, modifiche allo stato delle repliche di lettura, eventi di backup e ripristino, azioni di failover, eventi di errore, modifiche ai gruppi di sicurezza e molte altre notifiche. Ad esempio, se hai configurato un'istanza database di replica di lettura per fornire prestazioni e durata migliorate per il tuo database, ti consigliamo di monitorare gli eventi di Amazon RDS perleggi la replicacategoria di eventi associata alle istanze DB. Questo perché eventi come`RDS-EVENT-0057 Replication on the read replica was terminated`indica che la replica di lettura non è più sincronizzata con l'istanza database primaria. Una notifica al team responsabile che si è verificato un evento del genere potrebbe aiutare a mitigare tempestivamente il problema. AmazonEventBridgee servizi AWS aggiuntivi, comeAWS Lambda, Amazon Simple Queue Service (Amazon SQS) e Amazon Simple Notification Service (Amazon SNS) possono aiutarti ad automatizzare le risposte a eventi di sistema come problemi di disponibilità del database o modifiche delle risorse.

Sulla console Amazon RDS, puoi recuperare gli eventi delle ultime 24 ore. Se si utilizza ilAWS CLIo tramite l'API Amazon RDS per visualizzare gli eventi, puoi recuperare gli eventi degli ultimi 14 giorni utilizzando ildescrivi gli eventicomando come segue.

```
$ aws rds describe-events --source-identifier database-1 --source-type db-instance
{
    "Events": [
        {
            "SourceIdentifier": "database-1",
```

```
            "SourceType": "db-instance",
            "Message": "CloudWatch Logs Export enabled for logs [audit, error, general,
 slowquery]",
            "EventCategories": [],
            "Date": "2022-12-01T09:20:28.595000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        },
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "Finished updating DB parameter group",
            "EventCategories": [
                "configuration change"
            ],
            "Date": "2022-12-01T09:22:40.413000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        }
    ]
}
```

Se desideri archiviare gli eventi a lungo termine, fino al periodo di scadenza specificato o in modo permanente, puoi utilizzareCloudWatchRegistriper registrare le informazioni sugli eventi generati da Amazon RDS. Per implementare questa soluzione, puoi utilizzare un argomento di Amazon SNS per ricevere notifiche sugli eventi di Amazon RDS e quindi chiamare una funzione Lambda per accedere all'eventoCloudWatchTronchi.

1. Crea una funzione Lambda che verrà richiamata sull'evento e registra le informazioni dall'evento aCloudWatchTronchi. CloudWatchLogs è integrato con Lambda e fornisce un modo conveniente per registrare le informazioni sugli eventi, utilizzandostamparefunzione per`stdout`.
2. Crea un argomento SNS con un abbonamento a una funzione Lambda (setProtocollosu Lambda) e imposta ilPunto finaleall'Amazon Resource Name (ARN) della funzione Lambda che hai creato nel passaggio precedente.
3. Configura il tuo argomento SNS per ricevere notifiche sugli eventi Amazon RDS. Per istruzioni dettagliate, consulta laAWSArticolo re:postsu come far sì che il tuo argomento Amazon SNS riceva notifiche Amazon RDS.
4. Sulla console Amazon RDS, crea un nuovo abbonamento a un evento. SetObiettivoall'ARN, quindi seleziona l'argomento SNS che hai creato in precedenza. SetTipo di fonteeCategorie di eventi da includerein base alle vostre esigenze. Per ulteriori informazioni, vedereIscrizione alla notifica degli eventi Amazon RDSnella documentazione di Amazon RDS.

Log del database

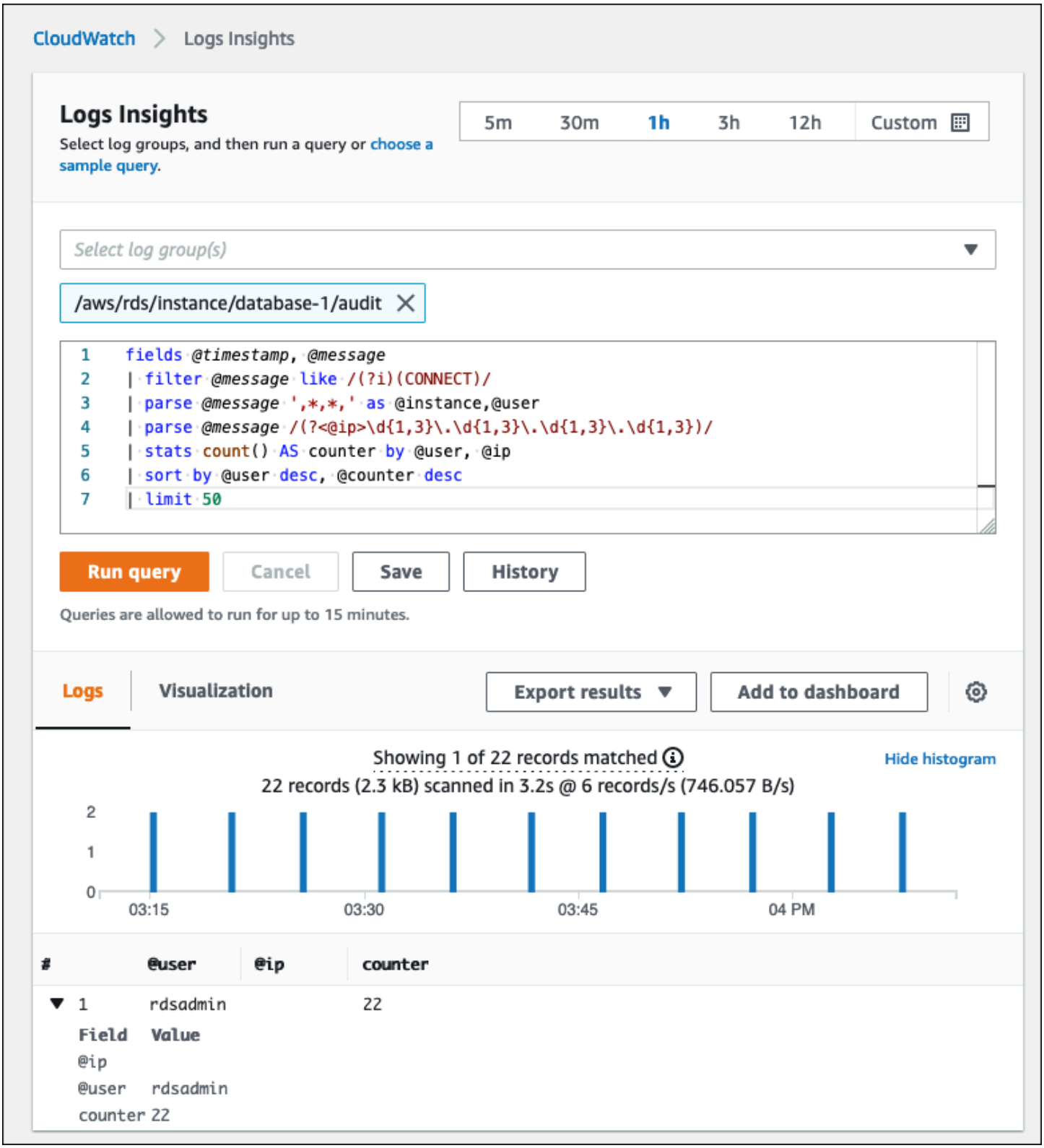
I database MySQL e MariaDB generano log a cui è possibile accedere per il controllo e la risoluzione dei problemi. Questi registri sono:

- Audit— L'audit trail è un insieme di record che registrano l'attività del server. Per ogni sessione client, registra chi si è connesso al server (nome utente e host), quali query sono state eseguite, a quali tabelle è stato effettuato l'accesso e quali variabili del server sono state modificate.
- Errore— Questo registro contiene il (`mysqld`) tempi di avvio e spegnimento e messaggi diagnostici come errori, avvisi e note che si verificano durante l'avvio e lo spegnimento del server e mentre il server è in esecuzione.
- Generale— Questo registro registra l'attività di`mysqld`, incluse le attività di connessione e disconnessione per ogni client e le query SQL ricevute dai client. Il registro generale delle interrogazioni può essere molto utile quando si sospetta un errore e si desidera sapere esattamente a cosa ha inviato il client`mysqld`.
- Interrogazione lenta— Questo registro fornisce una registrazione delle query SQL che hanno richiesto molto tempo per essere eseguite.

Come buona pratica, dovresti pubblicare log di database da Amazon RDS ad AmazonCloudWatchRegistri. ConCloudWatchRegistri, è possibile eseguire analisi in tempo reale dei dati di registro, archiviare i dati in uno storage altamente resistente e gestire i dati conCloudWatchAgente di log. Puoi accedi e controlla i log del tuo database dalla console Amazon RDS. Puoi anche usareCloudWatchLogs Insights per cercare e analizzare in modo interattivo i dati di log inCloudWatchTronchi. L'esempio seguente illustra una query nel registro di controllo che verifica quante volte`CONNECT`gli eventi vengono visualizzati nel registro, chi si è connesso e da quale client (indirizzo IP) si è connesso. L'estratto dal registro di controllo potrebbe avere il seguente aspetto:

```
20221201 14:07:05,ip-10-22-1-51,rdsadmin,localhost,821,0,CONNECT,,,0,SOCKET
20221201 14:07:05,ip-10-22-1-51,rdsadmin,localhost,821,0,DISCONNECT,,,0,SOCKET
20221201 14:12:20,ip-10-22-1-51,rdsadmin,localhost,822,0,CONNECT,,,0,SOCKET
20221201 14:12:20,ip-10-22-1-51,rdsadmin,localhost,822,0,DISCONNECT,,,0,SOCKET
20221201 14:17:35,ip-10-22-1-51,rdsadmin,localhost,823,0,CONNECT,,,0,SOCKET
20221201 14:17:35,ip-10-22-1-51,rdsadmin,localhost,823,0,DISCONNECT,,,0,SOCKET
20221201 14:22:50,ip-10-22-1-51,rdsadmin,localhost,824,0,CONNECT,,,0,SOCKET
20221201 14:22:50,ip-10-22-1-51,rdsadmin,localhost,824,0,DISCONNECT,,,0,SOCKET
```

L'esempio di query Log Insights mostra che `rdsadmin` connesso al database da `localhost` ogni 5 minuti, per un totale di 22 volte, come mostrato nella figura seguente. Questi risultati indicano che l'attività ha avuto origine da processi interni di Amazon RDS, come il sistema di monitoraggio stesso.



Gli eventi di registro spesso includono messaggi importanti che desideri contare, come avvisi o errori sulle operazioni associate alle istanze MySQL e MariaDB DB. Ad esempio, se un'operazione fallisce, può verificarsi un errore che viene registrato nel file di registro degli errori come segue:`ERROR 1114 (HY000): The table zip_codes is full`. Potresti voler monitorare queste voci per comprendere l'andamento dei tuoi errori. Puoicrea personalizzatoCloudWatchmetriche dai log di Amazon RDS utilizzando filtriper abilitare il monitoraggio automatico dei log del database Amazon RDS per monitorare un registro specifico per modelli specifici e generare un allarme in caso di violazioni del comportamento previsto. Ad esempio, crea un filtro metrico per il gruppo di log`/aws/rds/instance/database-1/error`che monitorerebbe il registro degli errori e cercherebbe ilmodello specifico, ad esempio`ERROR`. Imposta ilSchema di filtroa`ERROR`eValore metricoa`1`. Il filtro rileverà ogni record di registro che contiene la parola chiave`ERROR`e incrementerà il conteggio di 1 per ogni evento di registro che contiene «ERROR». Dopo aver creato il filtro, puoi impostare un allarme per avvisarti nel caso in cui vengano rilevati errori nel registro degli errori di MySQL o MariaDB.

Per ulteriori informazioni sul monitoraggio del log delle query lente e del registro degli errori, è possibile creare unCloudWatchdashboard e utilizzoCloudWatchLogs Insights, vedi il post sul blogCreare un'AmazonCloudWatchdashboard per monitorare Amazon RDS e Amazon Aurora MySQL.

Audit trail

L'audit trail (o registro di controllo) fornisce una registrazione cronologica rilevante per la sicurezza degli eventi nel tuo account AWS. Include eventi per Amazon RDS, che forniscono prove documentali della sequenza di attività che hanno interessato il tuo database o il tuo ambiente cloud. In Amazon RDS per MySQL o MariaDB, l'utilizzo dell'audit trail prevede:

- Monitoraggio del registro di controllo dell'istanza database
- Monitoraggio delle chiamate API Amazon RDS inAWS CloudTrail

Per un'istanza database Amazon RDS, gli obiettivi del controllo includono in genere:

- Abilitare la responsabilità per quanto segue:
  - Modifiche eseguite sul parametro o sulla configurazione di sicurezza
  - Azioni eseguite in uno schema, in una tabella o in una riga del database o azioni che influiscono su contenuti specifici

- Rilevamento e indagine sulle intrusioni
- Rilevamento e indagine di attività sospette
- Individuazione di problemi di autorizzazione; ad esempio, per identificare le violazioni dei diritti di accesso da parte di utenti regolari o privilegiati

L'audit trail del database cerca di rispondere a queste domande tipiche:Chi ha visualizzato o modificato i dati sensibili all'interno del tuo database? Quando è successo? Da dove ha avuto accesso ai dati un utente specifico? Gli utenti privilegiati hanno abusato dei loro diritti di accesso illimitati?

Sia MySQL che MariaDB implementano la funzione di audit trail delle istanze DB utilizzando il MariaDB Audit Plugin. Questo plugin registra le attività del database, come gli utenti che accedono al database e le query in esecuzione sul database. Il record con le attività del database è archiviato in un file di log. Per accedere al log di audit, l'istanza database deve usare un gruppo di opzioni personalizzato con l'opzione `MARIADB_AUDIT_PLUGIN`. Per ulteriori informazioni, vedereSupporto del plugin MariaDB Audit per MySQLnella documentazione di Amazon RDS. I record nel registro di controllo vengono archiviati in un formato specifico, come definito dal plugin. È possibile trovare ulteriori dettagli sul formato del registro di controllo nelDocumentazione di MariaDB Server.

LaCloud AWSaudit trail per il tuoAWSl'account è fornito dalAWS CloudTrailservizio. CloudTrailacquisisce le chiamate API per Amazon RDS come eventi. Tutte le azioni Amazon RDS vengono registrate. CloudTrailfornisce un registro delle azioni in Amazon RDS eseguite da un utente, da un ruolo o da un altroAWSservizio. Gli eventi comprendono le azioni intraprese nelAWSConsole di gestione,AWS CLI, eAWSSDK e API.

Esempio

In uno scenario di audit tipico, potrebbe essere necessario combinareAWS CloudTrailpercorsi con il registro di controllo del database e il monitoraggio degli eventi di Amazon RDS. Ad esempio, potresti avere uno scenario in cui i parametri del database della tua istanza database Amazon RDS (ad esempio,`database-1`) sono stati modificati e il tuo compito è identificare chi ha apportato la modifica, cosa è stato cambiato e quando è avvenuta la modifica.

Per eseguire l'operazione, segui questi passaggi:

1. Elenca gli eventi Amazon RDS che si sono verificati all'istanza del database`database-1`e determinare se c'è un evento nella categoria`configuration change`che ha il messaggio`Finished updating DB parameter group`.

```
$ aws rds describe-events --source-identifier database-1 --source-type db-instance
{
    "Events": [
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "Finished updating DB parameter group",
            "EventCategories": [
                "configuration change"
            ],
            "Date": "2022-12-01T09:22:40.413000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        }
    ]
}
```

2. Identifica il gruppo di parametri DB utilizzato dall'istanza database:

```
$ aws rds describe-db-instances --db-instance-identifier database-1 --query
 'DBInstances[*].[DBInstanceIdentifier,Engine,DBParameterGroups]'
[
    [
        "database-1",
        "mariadb",
        [
            {
                "DBParameterGroupName": "mariadb10-6-test",
                "ParameterApplyStatus": "pending-reboot"
            }
        ]
    ]
]
```

3. Usa ilAWS CLIda cercareCloudTraileventinella regione in cui`database-1`viene distribuito, nel periodo di tempo successivo all'evento Amazon RDS scoperto nella fase 1, e dove`EventName=ModifyDBParameterGroup`.

```
$ aws cloudtrail --region eu-west-3 lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=ModifyDBParameterGroup --start-time
 "2022-12-01, 09:00 AM" --end-time "2022-12-01, 09:30 AM"
```

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Role1",
                "accountId": "111122223333",
                "userName": "User1"
            }
        }
    },
    "eventTime": "2022-12-01T09:18:19Z",
    "eventSource": "rds.amazonaws.com",
    "eventName": "ModifyDBParameterGroup",
    "awsRegion": "eu-west-3",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "parameters": [
            {
                "isModifiable": false,
                "applyMethod": "pending-reboot",
                "parameterName": "innodb_log_buffer_size",
                "parameterValue": "8388612"
            },
            {
                "isModifiable": false,
                "applyMethod": "pending-reboot",
                "parameterName": "innodb_write_io_threads",
                "parameterValue": "8"
            }
        ],
        "dBParameterGroupName": "mariadb10-6-test"
    },
    "responseElements": {
        "dBParameterGroupName": "mariadb10-6-test"
    },
    "requestID": "fdf19353-de72-4d3d-bf29-751f375b6378",
    "eventID": "0bba7484-0e46-4e71-93a8-bd01ca8386fe",
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

LaCloudTraill'evento lo rivelaUser1con ruoloRole1daAWSl'account 111122223333 ha modificato il gruppo di parametri DBmariadb10-6-test, che è stato utilizzato dall'istanza DBdatabase-1sul2022-12-01 at 09:18:19 h. Due parametri sono stati modificati e impostati sui seguenti valori:

- innodb_log_buffer_size = 8388612
- innodb_write_io_threads = 8

AggiuntivoCloudTraileCloudWatchFunzionalità dei registri

Puoi risolvere gli incidenti operativi e di sicurezza negli ultimi 90 giorni visualizzandoCronologia degli eventisulCloudTrailconsolle. Per estendere il periodo di conservazione e sfruttare le funzionalità di interrogazione aggiuntive, è possibile utilizzareAWS CloudTrailLago. ConAWS CloudTrailInoltre, puoi conservare i dati degli eventi in un archivio dati degli eventi per un massimo di sette anni. Inoltre, il servizio supporta query SQL complesse che offrono una visualizzazione degli eventi più approfondita e personalizzabile rispetto alle visualizzazioni fornite dalle semplici ricerche chiave-valore inCronologia degli eventi.

Per monitorare gli audit trail, impostare allarmi e ricevere notifiche quando si verifica un'attività specifica, è necessario:configurareCloudTrailper inviare i registri delle tracce aCloudWatchRegistri. Dopo che i record del percorso sono stati archiviati comeCloudWatchLog, puoi definire filtri metrici per valutare gli eventi di registro in base a termini, frasi o valori e assegnare metriche ai filtri metrici. Inoltre, puoi creareCloudWatchallarmi generati in base alle soglie e ai periodi di tempo specificati. Ad esempio, puoi configurare allarmi che inviano notifiche ai team responsabili, in modo che possano intraprendere le azioni appropriate. Puoi anche configurare CloudWatch in modo che esegua automaticamente un'operazione in risposta a un allarme.

Avviso

Gli avvisi sono una delle fonti di informazioni più importanti per quanto riguarda la sicurezza, la disponibilità, le prestazioni e l'affidabilità dell'infrastruttura IT e dei servizi IT. Notificano e informano i team IT sulle minacce alla sicurezza in corso, sulle interruzioni, sui problemi di prestazioni o sui guasti del sistema.

L'Information Technology Infrastructure Library (ITIL), in particolare le pratiche di gestione dei servizi IT (ITSM), impostano gli avvisi automatici al centro del monitoraggio e della gestione degli eventi e delle migliori pratiche di gestione degli incidenti.

L'avviso di incidenti si verifica quando gli strumenti di monitoraggio generano avvisi per notificare al team e agli strumenti automatici (per elementi che sono automaticamente utilizzabili) in merito a modifiche, azioni ad alto rischio o guasti nell'ambiente IT. Gli avvisi IT sono la prima linea di difesa contro le interruzioni o le modifiche del sistema che possono trasformarsi in incidenti gravi. Monitorando automaticamente i sistemi e generando avvisi per interruzioni e modifiche rischiose, i team IT possono ridurre al minimo i tempi di inattività e i costi elevati che ne derivano.

Come best practice,AWSWell-Architected Framework prescrive cheusa il monitoraggio per generare notifiche basate sugli allarmi, emonitorare e allarmare in modo proattivo. UsoCloudWatcho un servizio di monitoraggio di terze parti per impostare allarmi che indicano quando le metriche superano i limiti previsti.

Lo scopo della gestione degli avvisi è stabilire procedure efficienti e standardizzate per la gestione di eventi e incidenti relativi all'IT attraverso la registrazione, la classificazione, la definizione e l'implementazione delle azioni, la chiusura e le attività di revisione post-incidente.

Sezioni

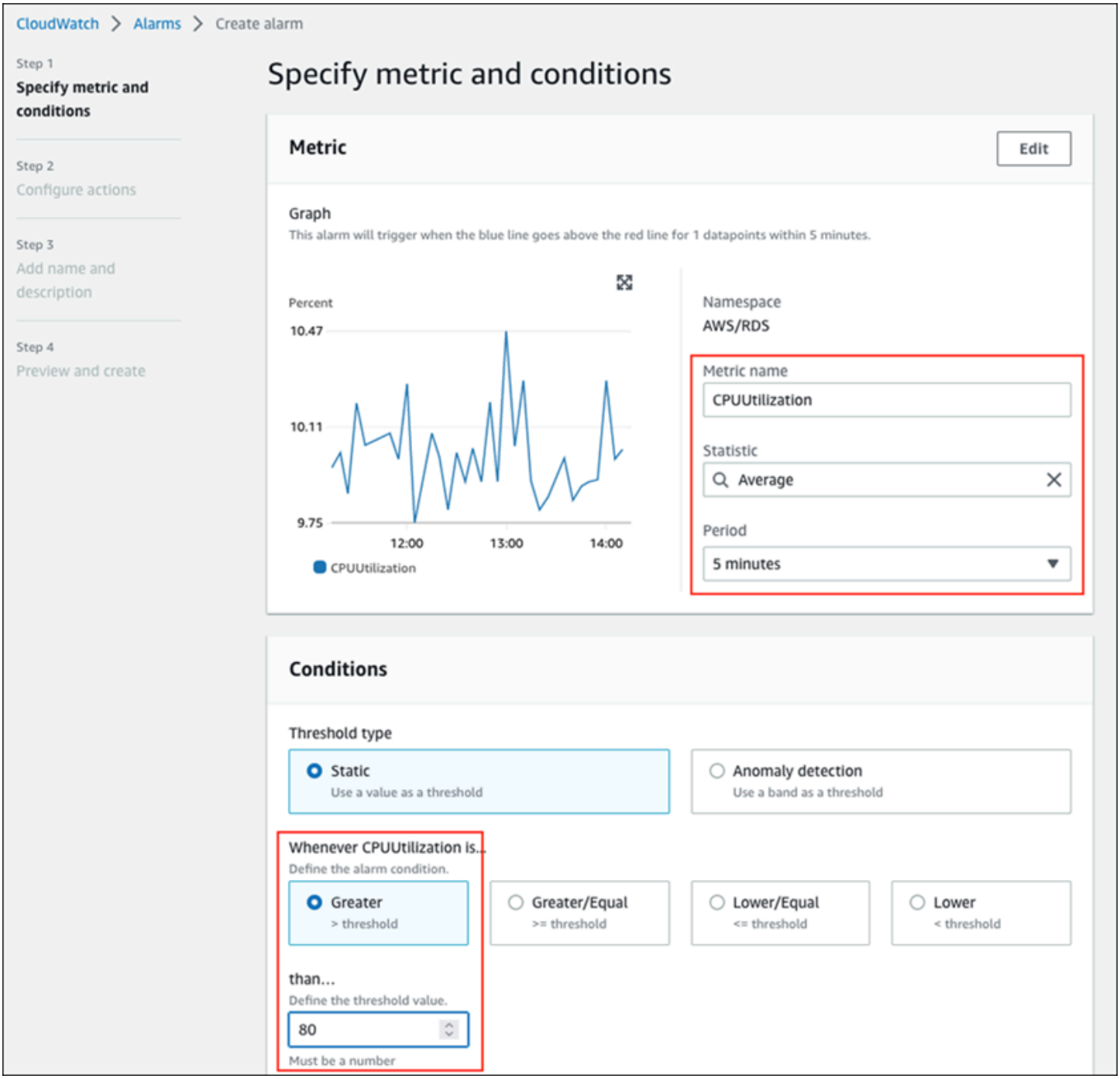
- Allarmi CloudWatch
- EventBridgeregole
- Specificazione di azioni, attivazione e disattivazione degli allarmi

Allarmi CloudWatch

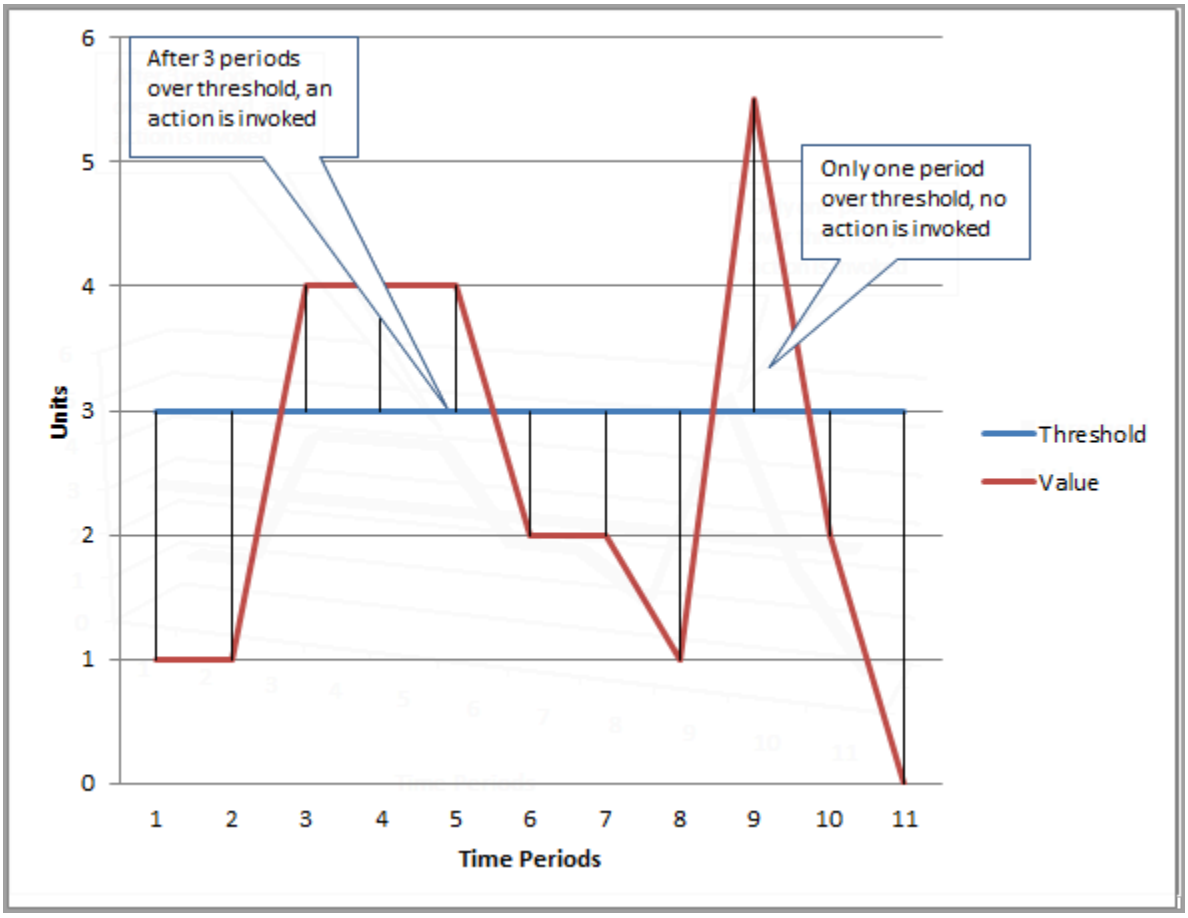
Quando gestisci le tue istanze database Amazon RDS, desideri monitorare e generare avvisi su diversi tipi di metriche, eventi e tracce. Per i database MySQL e MariaDB, le fonti di informazioni

critiche sonoMetriche delle istanze DB,Metriche del sistema operativo,eventi, registri e percorsi di controllo. Ti consigliamo di utilizzareCloudWatchallarmiper controllare una singola metrica in un periodo di tempo specificato.

L'esempio seguente illustra come è possibile impostare una sveglia che controlla il`CPUUtilization`metrica (percentuale di utilizzo della CPU) su tutte le istanze DB di Amazon RDS. L'allarme viene configurato in modo che venga attivato se l'utilizzo della CPU su qualsiasi istanza database è superiore all'80% per il periodo di valutazione di 5 minuti.



Ciò significa che l'allarme entra nel`ALARM`indica se uno dei tuoi database presenta un elevato utilizzo della CPU (oltre l'80%) per 5 minuti o più. L'allarme rimane nel`OK`stato se la CPU occasionalmente raggiunge un utilizzo superiore all'80% per un breve periodo di tempo e poi scende nuovamente al di sotto della soglia. Il grafico seguente illustra questa logica.



CloudWatchgli allarmi supportano allarmi metrici e compositi.

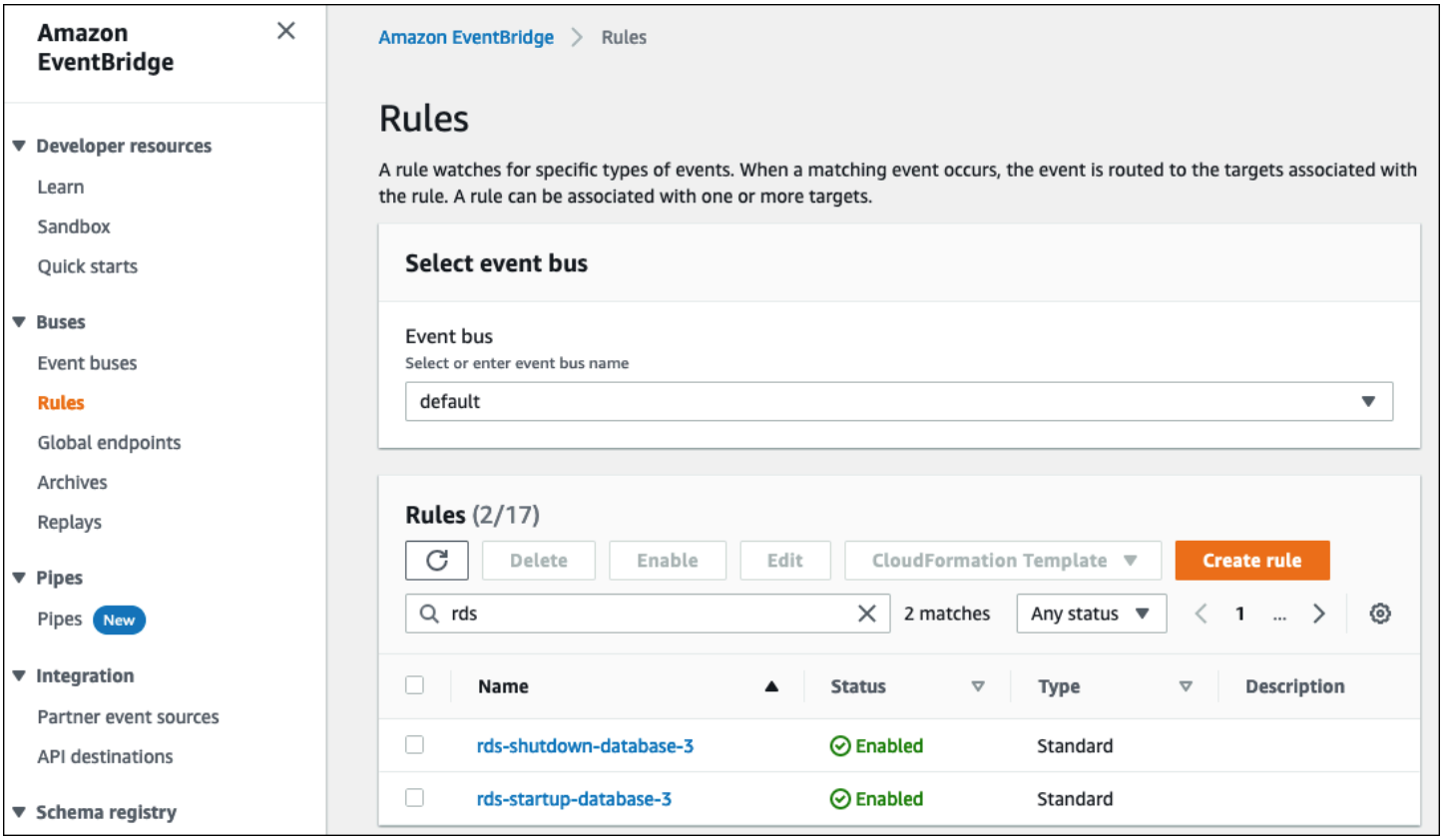
- UNallarme metricoorologi un singoloCloudWatchmetrico e può eseguire espressioni matematiche sulla metrica. Un allarme metrico può inviare messaggi Amazon SNS che, a loro volta, possono intraprendere una o più azioni in base al valore della metrica rispetto a una determinata soglia in un certo numero di periodi di tempo.
- UNallarme compositosi basa su un'espressione di regola, che valuta gli stati di più allarmi e inserisce`ALARM`dichiarare solo se sono soddisfatte tutte le condizioni della regola. Gli allarmi compositi vengono in genere utilizzati per ridurre il numero di avvisi non necessari. Ad esempio, potresti avere un allarme composito che contiene diversi allarmi metrici configurati per non eseguire mai azioni. L'allarme composito invierebbe un avviso quando tutti i singoli allarmi metrici nel composito sono già nel`ALARM`

CloudWatchgli allarmi possono solo guardareCloudWatchmetriche. Se desideri creare un avviso basato sull'errore, sulla query lenta o sui registri generali, devi creareCloudWatchmetriche dai log. Puoi farlo come discusso in precedenza nelmonitoraggio del sistema operativoeEventi,

registri e percorsi di controllosezioni, utilizzando filtri percreare metriche da eventi di registro. Allo stesso modo, per avvisare sulle metriche di Enhanced Monitoring, devi creare filtri metrici inCloudWatchdaCloudWatchTronchi.

Regole EventBridge

Eventi Amazon RDSvengono consegnati ad AmazonEventBridgee puoi usareEventBridgeregoleper reagire a tali eventi. Ad esempio, puoi creareEventBridgeregole che avvisano l'utente e intraprendono un'azione in caso di arresto o avvio di una specifica istanza database, come mostra la schermata seguente.

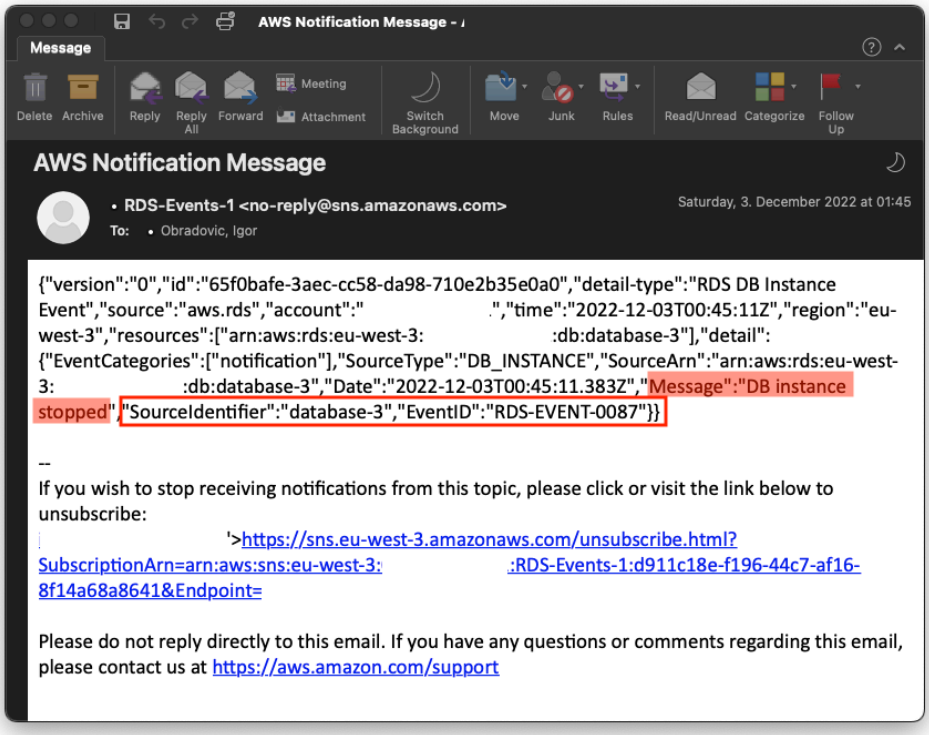


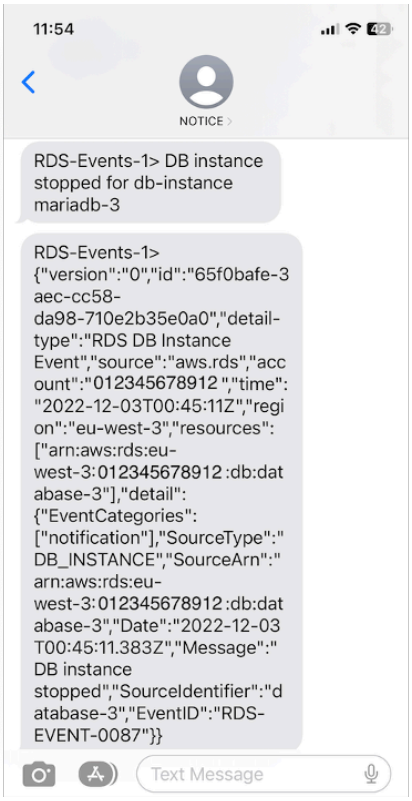
La regola che rilevaThe `DB instance has been stopped`l'evento ha l'ID evento Amazon RDS`RDS-EVENT-0087`, quindi hai impostato il`Event Pattern`proprietà della regola a:

```
{
  "source": ["aws.rds"],
  "detail-type": ["RDS DB Instance Event"],
  "detail": {
    "SourceArn": ["arn:aws:rds:eu-west-3:111122223333:db:database-3"],
    "EventID": ["RDS-EVENT-0087"]
```

```
  }
}
```

Questa regola monitora l'istanza database`database-3`solo, e orologi per`RDS-EVENT-0087`evento. QuandoEventBridgerileva l'evento, lo invia a una risorsa o a un endpoint, noto comebersaglio. Qui puoi specificare l'azione che desideri eseguire se l'istanza Amazon RDS si spegne. Puoi inviare l'evento a molti possibili destinatari, tra cui un argomento SNS, una coda Amazon Simple Queue Service (Amazon SQS),AWS Lambdafunzione,AWS Systems ManagerAutomazione, unAWS Batchjob, Amazon API Gateway, un piano di risposta in Incident Manager, una funzionalità diAWS Systems Managere molti altri ancora. Ad esempio, è possibile creare un argomento SNS che invierà un'e-mail di notifica e un SMS e assegnare tale argomento SNS come destinazione delEventBridgeregola. Se l'istanza database Amazon RDS`database-3`è stato interrotto, Amazon RDS consegna l'evento`RDS-EVENT-0087`aEventBridge, dove viene rilevato. EventBridgequindi chiama il target, che è l'argomento SNS. L'argomento SNS è configurato per inviare un'e-mail (come mostrato nella figura seguente) e un SMS.





Specificazione di azioni, attivazione e disattivazione degli allarmi

Puoi usare unCloudWatchallarme per specificare quali azioni deve intraprendere l'allarme quando passa da un`OK`,`ALARM`, e`INSUFFICIENT_DATA`stati. CloudWatchha un'integrazione integrata con

gli argomenti SNS e diverse categorie di azioni aggiuntive che non sono applicabili ai parametri di Amazon RDS, come le azioni Amazon Elastic Compute Cloud (Amazon EC2) o le azioni di gruppo Amazon EC2 Auto Scaling. EventBridgeviene generalmente utilizzato per scrivere regole e definire obiettivi che intraprendono azioni quando viene attivato l'allarme per le metriche di Amazon RDS. CloudWatchinvia eventi aEventBridgeogni volta aCloudWatchl'allarme cambia il suo stato. È possibile utilizzare questi eventi di modifica dello stato di allarme per attivare un evento target inEventBridge. Per ulteriori informazioni, vedereEventi di allarme eEventBridgenelCloudWatchdocumentazione.

Potrebbe anche essere necessario gestire gli allarmi; ad esempio, disattivare automaticamente un allarme durante le modifiche o i test di configurazione pianificati e quindi riattivare l'allarme al termine dell'azione pianificata. Ad esempio, se hai un aggiornamento pianificato e pianificato del software del database che richiede tempi di inattività e disponi di allarmi che verranno attivati se il database non sarà più disponibile, puoi disabilitare e abilitare gli allarmi utilizzando le azioni APIDisableAlarmActionseEnableAlarmActions, o ildisable-alarm-actionseenable-alarm-actionscomandi inAWS CLI. È inoltre possibile visualizzare la cronologia degli allarmi sulCloudWatchconsole o utilizzando ilDescribeAlarmHistoryAzione API odescribe-alarm-historycomando nelAWS CLI. CloudWatch conserva la cronologia dell'allarme per due settimane. SulCloudWatchconsole, puoi scegliere ilPreferiti e recentimenu nel riquadro di navigazione per impostare e accedere agli allarmi preferiti e visitati più di recente.

Risorse e passaggi successivi

Per ulteriori informazioni sulla migrazione dei database relazionali versoCloud AWS, vedi la seguente strategia sulAWSSito web dedicato alle linee guida prescrittive:

- Strategia di migrazione per database relazionali

Puoi esploraremodelli di migrazione del databaseperstep-by-stepistruzioni relative ai database relazionali specifici in esecuzione nelCloud AWS, comprese le attività relative al monitoraggio, alla migrazione e alla gestione dei dati.

Usa i filtri in quella pagina per trovare i modelli in base aAWSservizio (ad esempio, migrazioni ad Amazon RDS o Amazon Aurora), per carico di lavoro (ad esempio open source, che include database MySQL e MariaDB) o per uso pianificato (produzione o progetto pilota).

Per ulteriori risorse, consulta quanto segue:

- Guida per l'utente di Amazon Relational Database Service
- AmazonCloudWatchGuida per l'utente
- Domande frequenti su Amazon RDS
- Domande frequenti su Performance Insights
- Fornisci i contatori di Amazon RDS Performance Insights a un fornitore terzo di servizi di monitoraggio delle prestazioni delle applicazioni tramite AmazonCloudWatchFlusso di metriche(AWSpost sul blog)
- Creare un'AmazonCloudWatchdashboard per monitorare Amazon RDS e Amazon Aurora MySQL(AWSpost sul blog)
- Ottimizzazione di Amazon RDS per MySQL con Performance Insights(AWSpost sul blog)

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
Informazioni aggiornate	Sono state aggiornate le informazioni sugli esportatori e sono state aggiunte le linee guida per la scelta di un esportatore.	13 giugno 2024
Pubblicazione iniziale	—	30 giugno 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 disturbare o causare danni a individui o organizzazioni.

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

Un sistema che memorizza per primo il byte più importante. Vedi anche endianness.

Classificazione binaria

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

filtro Bloom

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

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 AWS servizio 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, puoi utilizzarlo AWS CloudFormation per rilevare la deriva nelle risorse di sistema oppure puoi usarlo AWS Control Tower per rilevare cambiamenti nella tua landing zone che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

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

AWS servizi 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 `WHERE`. `true` `false`

predicato pushdown

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

controllo preventivo

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

principale

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

Privacy fin dalla progettazione

Un approccio 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 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 utilizzare Regioni AWS il proprio 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. AWS servizio

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 AWS servizio. Puoi utilizzare l'endpoint per connetterti a livello di programmazione al servizio di destinazione. Per ulteriori informazioni, consulta Endpoint del AWS servizio 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.