Progettazione e implementazione di registrazione e monitoraggio con Amazon CloudWatch

# AWS Guida prescrittiva

# AWS Guida prescrittiva: Progettazione e implementazione di registrazione e monitoraggio con Amazon CloudWatch

# Table of Contents

# Progettazione e implementazione della registrazione e del monitoraggio con Amazon CloudWatch

Khurram Nizami, Amazon Web Services ()AWS

Aprile 2023 (cronologia dei documenti)

Questa guida ti aiuta a progettare e implementare la registrazione e il monitoraggio con Amazon CloudWatch e i relativi servizi di gestione e governance di Amazon Web Services (AWS) per carichi di lavoro che utilizzano istanze Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), e server locali. AWS Lambda La guida è destinata ai team operativi, agli ingegneri e agli DevOps ingegneri delle applicazioni che gestiscono i carichi di lavoro sul cloud. AWS

Il tuo approccio alla registrazione e al monitoraggio dovrebbe basarsi sui sei pilastri del Well-Architected AWS Framework. Questi pilastri sono l'eccellenza operativa, la sicurezza, l'affidabilità, l'efficienza delle prestazioni e l'ottimizzazione dei costi. Una soluzione di monitoraggio e allarme ben progettata migliora l'affidabilità e le prestazioni aiutandovi ad analizzare e adattare in modo proattivo l'infrastruttura.

Questa guida non tratta ampiamente la registrazione e il monitoraggio per la sicurezza o l'ottimizzazione dei costi, poiché si tratta di argomenti che richiedono una valutazione approfondita. Esistono molti AWS servizi che supportano la registrazione e il monitoraggio della sicurezza, tra cui Amazon Inspector AWS CloudTrailAWS Config, AmazonDetective, AmazonMacie, Amazon e. GuardDuty AWS Security Hub CSPM Puoi anche utilizzare AWS Cost Exploreri parametri di fatturazione e di CloudWatch fatturazione per l'ottimizzazione dei costi. Budget AWS

La tabella seguente descrive le sei aree che la soluzione di registrazione e monitoraggio dovrebbe affrontare.

| | |
|---|---|
| Acquisizione e acquisizione di file di registro e metriche | Identifica, configura e invia log e metriche di sistema e applicazioni a servizi da fonti diverse. AWS |
| Ricerca e analisi dei log | Cerca e analizza i log per la gestione delle operazioni, l'identificazione dei problemi, |

| | |
|---|---|
| | la risoluzione dei problemi e l'analisi delle applicazioni. |
| Monitoraggio delle metriche e allarmi | Identifica e agisci in base alle osservazioni e alle tendenze dei tuoi carichi di lavoro. |
| Monitoraggio della disponibilità di applicazioni e servizi | Riduci i tempi di inattività e migliora la capacità di soddisfare gli obiettivi dei livelli di servizio monitorando continuamente la disponibilità del servizio. |
| Applicazioni di tracciamento | Tieni traccia delle richieste delle applicazioni nei sistemi e nelle dipendenze esterne per ottimizzare le prestazioni, eseguire l'analisi delle cause principali e risolvere i problemi. |
| Creazione di dashboard e visualizzazioni | Crea dashboard incentrate su metriche e osservazioni pertinenti per i tuoi sistemi e carichi di lavoro, il che aiuta il miglioram ento continuo e l'individuazione proattiva dei problemi. |

CloudWatch può soddisfare la maggior parte dei requisiti di registrazione e monitoraggio e fornisce una soluzione affidabile, scalabile e flessibile. Molti AWS servizi forniscono automaticamente le CloudWatch metriche, oltre all'integrazione della CloudWatch registrazione per il monitoraggio e l'analisi. CloudWatch fornisce inoltre agenti e driver di registro per supportare una varietà di opzioni di elaborazione come server (sia nel cloud che in locale), contenitori e elaborazione serverless. Questa guida copre anche i seguenti AWS servizi utilizzati per la registrazione e il monitoraggio:

- AWS Systems Manager Distributore, Systems Manager State Manager e Systems Manager Automation per automatizzare, configurare e aggiornare l' CloudWatch agente per le istanze EC2 e i server locali
- Amazon OpenSearch Service per l'aggregazione, la ricerca e l'analisi avanzate dei log
- Controlli dello stato di Amazon Route 53 e CloudWatchSynthetics per monitorare la disponibilità di applicazioni e servizi

- Amazon Managed Service for Prometheus per il monitoraggio di applicazioni containerizzate su larga scala
- AWS X-Rayper il tracciamento delle applicazioni e l'analisi del runtime
- Amazon Managed Grafana per visualizzare e analizzare i dati da più fonti (ad esempio, CloudWatch Amazon OpenSearch Service e Amazon Timestream)

I servizi di AWS elaborazione che scegli influiscono anche sull'implementazione e la configurazione della tua soluzione di registrazione e monitoraggio. Ad esempio, l'implementazione e CloudWatch la configurazione sono diverse per Amazon EC2, Amazon ECS, Amazon EKS e Lambda.

I proprietari di applicazioni e carichi di lavoro possono spesso dimenticare la registrazione e il monitoraggio o configurarli e implementarli in modo incoerente. Ciò significa che i carichi di lavoro entrano in produzione con un'osservabilità limitata, il che causa ritardi nell'identificazione dei problemi e aumenta il tempo necessario per risolverli e risolverli. Come minimo, la soluzione di registrazione e monitoraggio deve riguardare il livello di sistema per i log e le metriche a livello di sistema operativo (OS), oltre al livello applicativo per i log e le metriche delle applicazioni. La guida fornisce un approccio consigliato per affrontare questi due livelli in diversi tipi di elaborazione, inclusi i tre tipi di elaborazione descritti nella tabella seguente.

| | |
|---|---|
| Istanze EC2 immutabili e a lunga durata | Registri e metriche di sistema e applicazioni su più sistemi operativi () OSs in più regioni o account. AWS |
| Container | Registri e parametri di sistema e applicazioni per i cluster Amazon ECS e Amazon EKS, inclusi esempi per diverse configurazioni. |
| Serverless | Registri e metriche di sistema e applicazioni per le funzioni Lambda e considerazioni sulla personalizzazione. |

Questa guida fornisce una soluzione di registrazione e monitoraggio che riguarda i servizi correlati AWS nelle CloudWatch seguenti aree:

- Pianificazione dell' CloudWatch implementazione— Considerazioni per la pianificazione dell' CloudWatch implementazione e indicazioni sulla centralizzazione della configurazione. CloudWatch

- Configurazione dell' CloudWatch agente per le istanze EC2 e i server locali— dettagli CloudWatch di configurazione per la registrazione e le metriche a livello di sistema e di applicazione.
- CloudWatch approcci di installazione di agenti per Amazon EC2 e server locali— Approcci per l'installazione dell' CloudWatch agente, inclusa la distribuzione automatizzata tramite Systems Manager su più regioni e account.
- Registrazione e monitoraggio su Amazon ECS— Linee guida per la configurazione CloudWatch di log e parametri a livello di cluster e di applicazione in Amazon ECS.
- Registrazione e monitoraggio su Amazon EKS— Linee guida per la configurazione CloudWatch di log e parametri a livello di cluster e di applicazione in Amazon EKS.
- Monitoraggio di Prometheus su Amazon EKS— Presenta e confronta Amazon Managed Service for Prometheus con il monitoraggio di Container Insights per Prometheus. CloudWatch
- Registrazione e metriche per AWS Lambda— Guida per la configurazione delle CloudWatch funzioni Lambda.
- Ricerca e analisi dei log in CloudWatch— Metodi per analizzare i log utilizzando Amazon CloudWatch Application Insights, CloudWatch Logs Insights ed estendere l'analisi dei log ad Amazon Service. OpenSearch
- Opzioni allarmanti con CloudWatch— Introduce il rilevamento di CloudWatch allarmi e CloudWatch anomalie e fornisce indicazioni sulla creazione e la configurazione degli allarmi.
- Monitoraggio della disponibilità di applicazioni e servizi— Introduce e confronta i controlli di integrità di CloudWatch Synthetics e Route 53 per il monitoraggio automatizzato della disponibilità.
- Tracciamento delle applicazioni con AWS X-Ray— Introduzione e configurazione per il tracciamento delle applicazioni utilizzando X-Ray per Amazon EC2, Amazon ECS, Amazon EKS e Lambda
- Dashboard e visualizzazioni con CloudWatch— Introduzione ai CloudWatch dashboard per una migliore osservabilità tra i carichi di lavoro. AWS
- CloudWatch integrazione con AWS i servizi— Spiega come si CloudWatch integra con vari servizi. AWS
- Amazon Managed Grafana per dashboard e visualizzazione— Presenta e confronta Amazon Managed Grafana con CloudWatch per dashboard e visualizzazione.

In questa guida vengono utilizzati esempi di implementazione in queste aree e sono disponibili anche nell'archivio Samples.AWS GitHub

# Obiettivi aziendali specifici

La creazione di una soluzione di registrazione e monitoraggio progettata per il AWS cloud è fondamentale per ottenere i sei vantaggi del cloud computing. La soluzione di registrazione e monitoraggio dovrebbe aiutare l'organizzazione IT a raggiungere risultati aziendali a vantaggio dei processi aziendali, dei partner commerciali, dei dipendenti e dei clienti. Dopo l'implementazione di una soluzione di registrazione e monitoraggio allineata al Well-Architected AWS Framework, è possibile aspettarsi i seguenti quattro risultati:

## Accelera la prontezza operativa

L'abilitazione di una soluzione di registrazione e monitoraggio è un componente importante della preparazione di un carico di lavoro per il supporto e l'utilizzo in produzione. La prontezza operativa può rapidamente diventare un ostacolo se ci si affida troppo ai processi manuali e può anche ridurre il time to value (TTV) per gli investimenti IT. Un approccio inefficace si traduce anche in una limitata osservabilità dei carichi di lavoro. Ciò può aumentare il rischio di interruzioni prolungate, insoddisfazione dei clienti e fallimento dei processi aziendali.

Puoi utilizzare gli approcci di questa guida per standardizzare e automatizzare la registrazione e il monitoraggio sul cloud. AWS I nuovi carichi di lavoro richiedono quindi una preparazione e un intervento manuali minimi per la registrazione e il monitoraggio della produzione. Ciò aiuta anche a ridurre i tempi e i passaggi necessari per creare standard di registrazione e monitoraggio su larga scala per diversi carichi di lavoro su più account e regioni.

## Migliora l'eccellenza operativa

Questa guida fornisce diverse best practice per la registrazione e il monitoraggio che aiutano carichi di lavoro diversi a raggiungere gli obiettivi aziendali e l'eccellenza operativa. Questa guida fornisce anche esempi dettagliati e modelli open source riutilizzabili che è possibile utilizzare con un approccio Infrastructure as Code (IaC) per implementare una soluzione di registrazione e monitoraggio ben architettata utilizzando i servizi. AWS Il miglioramento dell'eccellenza operativa è iterativo e richiede un miglioramento continuo. La guida fornisce suggerimenti su come migliorare continuamente le pratiche di registrazione e monitoraggio.

# Migliora la visibilità operativa

I processi e le applicazioni aziendali potrebbero essere supportati da diverse risorse IT e ospitati su diversi tipi di elaborazione, in locale o sul AWS cloud. La visibilità operativa può essere limitata da implementazioni incoerenti e incomplete della strategia di registrazione e monitoraggio. L'adozione di un approccio completo di registrazione e monitoraggio consente di identificare, diagnosticare e rispondere rapidamente ai problemi relativi ai carichi di lavoro. Questa guida aiuta a progettare e implementare approcci per migliorare la visibilità operativa completa e ridurre gli errori nel tempo medio di risoluzione (MTTR). Un approccio completo di registrazione e monitoraggio aiuta inoltre l'organizzazione a migliorare la qualità del servizio, migliorare l'esperienza dell'utente finale e rispettare gli accordi sui livelli di servizio (). SLAs

# Scalate le operazioni e riducete i costi generali

Puoi scalare le pratiche di registrazione e monitoraggio riportate in questa guida per supportare più regioni e account, risorse di breve durata e più ambienti. La guida fornisce approcci ed esempi per automatizzare le fasi manuali (ad esempio installazione e configurazione degli agenti, monitoraggio delle metriche e notifica o azione in caso di problemi). Questi approcci sono utili quando l'adozione del cloud matura e cresce ed è necessario scalare la capacità operativa senza aumentare le attività o le risorse di gestione del cloud.

# Pianificazione dell' CloudWatch implementazione

La complessità e la portata di una soluzione di registrazione e monitoraggio dipendono da diversi fattori, tra cui:

- Quanti ambienti, regioni e account vengono utilizzati e in che modo questo numero potrebbe aumentare.
- La varietà e i tipi di carichi di lavoro e architetture esistenti.
- I tipi e i tipi di elaborazione devono essere OSs registrati e monitorati.
- Se ci sono sia sedi che infrastrutture locali. AWS
- I requisiti di aggregazione e analisi di più sistemi e applicazioni.
- Requisiti di sicurezza che impediscono l'esposizione non autorizzata di log e metriche.
- Prodotti e soluzioni che devono integrarsi con la vostra soluzione di registrazione e monitoraggio per supportare i processi operativi.

È necessario rivedere e aggiornare regolarmente la soluzione di registrazione e monitoraggio con implementazioni di carichi di lavoro nuove o aggiornate. Gli aggiornamenti alla registrazione, al monitoraggio e agli allarmi devono essere identificati e applicati quando si riscontrano problemi. Questi problemi possono quindi essere identificati in modo proattivo e prevenuti in futuro.

È necessario assicurarsi di installare e configurare in modo coerente software e servizi per l'acquisizione e l'acquisizione di log e metriche. Un approccio consolidato di registrazione e monitoraggio utilizza servizi e soluzioni di fornitori di software diversi AWS o indipendenti (ISV) per diversi domini (ad esempio sicurezza, prestazioni, rete o analisi). Ogni dominio ha i propri requisiti di distribuzione e configurazione.

Si consiglia di CloudWatch utilizzarlo per acquisire e inserire log e metriche per diversi OSs tipi di elaborazione. Molti AWS servizi lo utilizzano CloudWatch per registrare, monitorare e pubblicare log e metriche, senza richiedere ulteriori configurazioni. CloudWatch fornisce un agente software che può essere installato e configurato per diversi ambienti OSs . Le seguenti sezioni descrivono come distribuire, installare e configurare l' CloudWatch agente per più account, regioni e configurazioni:

Argomenti

# Utilizzo CloudWatch in account centralizzati o distribuiti

Sebbene CloudWatch sia progettato per monitorare AWS servizi o risorse in un unico account e regione, è possibile utilizzare un account centrale per acquisire registri e metriche da più account e regioni. Se utilizzi più di un account o di una regione, dovresti valutare se utilizzare l'approccio centralizzato dell'account o un singolo account per acquisire log e metriche. In genere, è necessario un approccio ibrido per le implementazioni con più account e più regioni per supportare i requisiti di sicurezza, analisi, operazioni e proprietari dei carichi di lavoro.

La tabella seguente fornisce le aree da considerare quando si sceglie di utilizzare un approccio centralizzato, distribuito o ibrido.

| | |
|---|---|
| Strutture degli account | L'organizzazione potrebbe avere diversi account separati (ad esempio, account per carichi di lavoro non di produzione e di produzione) o migliaia di account per singole applicazioni in ambienti specifici. Ti consigliamo di conservare i log e le metriche delle applicazioni nell'account su cui viene eseguito il carico di lavoro, in modo da consentire ai proprietari dei carichi di lavoro di accedere ai log e alle metriche. Ciò consente loro di svolgere un ruolo attivo nella registrazione e nel monitoraggio. Si consiglia inoltre di utilizzar e un account di registrazione separato per aggregare tutti i registri dei carichi di lavoro per analisi, aggregazione, tendenze e operazion i centralizzate. È inoltre possibile utilizzare account di registrazione separati per la sicurezza, l'archiviazione, il monitoraggio e l'analisi. |
| Requisiti di accesso | I membri del team (ad esempio, i proprietari dei carichi di lavoro o gli sviluppatori) richiedono l'accesso a log e metriche per risolvere i problemi e apportare miglioramenti. I log devono essere conservati nell'account del carico di lavoro per facilitare l'accesso e la risoluzio ne dei problemi. Se i log e le metriche vengono conservati in un account separato dal carico di lavoro, gli utenti potrebbero dover alternare regolarmente gli account.<br><br>L'utilizzo di un account centralizzato fornisce informazioni di registro agli utenti autorizzati senza concedere l'accesso all'account del carico di lavoro. Ciò può semplificare i requisiti di accesso per i |

| | |
|---|---|
| | carichi di lavoro analitici in cui è richiesta l'aggregazione dei carichi di lavoro eseguiti su più account. L'account di registrazione centralizzato può anche avere opzioni di ricerca e aggregazione alternative, come un cluster Amazon OpenSearch Service. Amazon OpenSearch Service fornisce un controllo granulare degli accessi ai log fino al livello di campo. Un controllo granulare degli accessi è importante quando si dispone di dati sensibili o riservati che richiedono accessi e autorizzazioni specializzati. |
| Operazioni | Molte organizzazioni dispongono di un team operativo e di sicurezza centralizzato o di un'organizzazione esterna per il supporto operativo che richiede l'accesso ai registri per il monitoraggio. La registrazione e il monitoraggio centralizzati possono semplificare l'identificazione delle tendenze, la ricerca, l'aggregazione e l'esecuzione di analisi su tutti gli account e i carichi di lavoro. Se la tua organizzazione utilizza l'approccio «tu lo costruisci, lo esegui» DevOps, i proprietari dei carichi di lavoro devono registrare e monitorare le informazioni nel proprio account. Potrebbe essere necessario un approccio ibrido per soddisfare le operazioni e l'analisi centrali, oltre alla proprietà distribuita dei carichi di lavoro. |
| Ambiente | Puoi scegliere di ospitare log e metriche in una posizione centrale per gli account di produzione e conservare log e metriche per altri ambienti (ad esempio, sviluppo o test) nello stesso account o in account separati, a seconda dei requisiti di sicurezza e dell'architettura dell'account. Questo aiuta a impedire l'accesso ai dati sensibili creati durante la produzione da parte di un pubblico più ampio. |

CloudWatch offre diverse opzioni per elaborare i log in tempo reale con filtri di CloudWatch abbonamento. È possibile utilizzare i filtri di abbonamento per trasmettere i log in tempo reale a AWS servizi per l'elaborazione, l'analisi e il caricamento personalizzati su altri sistemi. Ciò può essere particolarmente utile se si adotta un approccio ibrido in cui i log e le metriche sono disponibili in

singoli account e regioni, oltre a un account e una regione centralizzati. L'elenco seguente fornisce esempi di AWS servizi che possono essere utilizzati a tale scopo:

- Amazon Data Firehose — Firehose fornisce una soluzione di streaming che si ridimensiona e si ridimensiona automaticamente in base al volume di dati prodotto. Non è necessario gestire il numero di shard in un flusso di dati Amazon Kinesis e puoi connetterti direttamente ad Amazon Simple Storage Service (Amazon S3) OpenSearch , Amazon Service o Amazon Redshift senza codifica aggiuntiva. Firehose è una soluzione efficace se si desidera centralizzare i log in tali servizi. AWS
- Amazon Kinesis Data Streams — Kinesis Data Streams è una soluzione appropriata se è necessario integrarsi con un servizio che Firehose non supporta e implementare una logica di elaborazione aggiuntiva. Puoi creare una destinazione Amazon CloudWatch Logs nei tuoi account e nelle tue regioni che specifichi un flusso di dati Kinesis in un account centrale e un ruolo AWS Identity and Access Management (IAM) che gli conceda l'autorizzazione a inserire record nel flusso. Kinesis Data Streams offre una landing zone flessibile e aperta per i dati di registro, che possono poi essere utilizzati da diverse opzioni. Puoi leggere i dati di registro di Kinesis Data Streams nel tuo account, eseguire la preelaborazione e inviare i dati alla destinazione prescelta.

  Tuttavia, è necessario configurare gli shard per lo stream in modo che abbia le dimensioni appropriate per i dati di registro prodotti. Kinesis Data Streams funge da intermediario o coda temporanea per i dati di registro e puoi archiviare i dati all'interno del flusso Kinesis per un periodo compreso tra uno e 365 giorni. Kinesis Data Streams supporta anche la funzionalità di replay, il che significa che puoi riprodurre dati che non sono stati consumati.
- Amazon OpenSearch Service: CloudWatch i log possono trasmettere i log di un gruppo di log a un OpenSearch cluster in un account individuale o centralizzato. Quando si configura un gruppo di log per lo streaming di dati verso un OpenSearch cluster, viene creata una funzione Lambda nello stesso account e nella stessa regione del gruppo di log. La funzione Lambda deve disporre di una connessione di rete con il OpenSearch cluster. Puoi personalizzare la funzione Lambda per eseguire una preelaborazione aggiuntiva, oltre a personalizzare l'inserimento in Amazon Service. OpenSearch La registrazione centralizzata con Amazon OpenSearch Service semplifica l'analisi, la ricerca e la risoluzione dei problemi tra più componenti della tua architettura cloud.
- Lambda: se utilizzi Kinesis Data Streams, devi fornire e gestire le risorse di calcolo che consumano i dati del tuo stream. Per evitare ciò, puoi trasmettere i dati di registro direttamente a Lambda per l'elaborazione e inviarli a una destinazione in base alla tua logica. Ciò significa che non è necessario fornire e gestire le risorse di calcolo per elaborare i dati in arrivo. Se scegli di utilizzare Lambda, assicurati che la tua soluzione sia compatibile con le quote Lambda.

Potrebbe essere necessario elaborare o condividere i dati di registro memorizzati in CloudWatch Logs in formato file. Puoi creare un'attività di esportazione per esportare un gruppo di log in Amazon S3 per una data o un intervallo di tempo specifico. Ad esempio, puoi scegliere di esportare i log su base giornaliera in Amazon S3 per analisi e audit. Lambda può essere utilizzata per automatizzare questa soluzione. Puoi anche combinare questa soluzione con la replica di Amazon S3 per spedire e centralizzare i log da più account e regioni a un unico account e regione centralizzati.

La configurazione CloudWatch dell'agente può anche specificare un `credentials` campo nella sezione. `agent` Questo specifica un ruolo IAM da utilizzare per l'invio di metriche e log a un account diverso. Se specificato, questo campo contiene il parametro. `role_arn` Questo campo può essere utilizzato quando sono necessari solo la registrazione e il monitoraggio centralizzati in un account e in una regione centralizzati specifici.

Puoi anche utilizzare AWS SDK per scrivere la tua applicazione di elaborazione personalizzata in una lingua a tua scelta, leggere i log e le metriche dei tuoi account e inviare dati a un account centralizzato o a un'altra destinazione per ulteriori elaborazioni e monitoraggio.

## Gestione dei file di configurazione dell'agente CloudWatch

Ti consigliamo di creare una configurazione standard CloudWatch dell'agente Amazon che includa i log di sistema e i parametri che desideri acquisire su tutte le istanze Amazon Elastic Compute Cloud (Amazon EC2) e i server locali. Puoi utilizzare la procedura guidata del file di configurazione dell' CloudWatch agente per aiutarti a creare il file di configurazione. È possibile eseguire la procedura guidata di configurazione più volte per generare configurazioni uniche per sistemi e ambienti diversi. È inoltre possibile modificare il file di configurazione o creare varianti utilizzando lo schema del file di configurazione. Il file di configurazione CloudWatch dell'agente può essere archiviato nei parametri di AWS Systems Manager Parameter Store. Puoi creare parametri Parameter Store separati se disponi di più file di configurazione degli CloudWatch agenti. Se utilizzi più account AWS o regioni AWS, devi gestire e aggiornare i parametri di Parameter Store in ogni account e regione. In alternativa, puoi gestire centralmente le CloudWatch configurazioni come file in Amazon S3 o uno strumento di controllo delle versioni a tua scelta.

Lo `amazon-cloudwatch-agent-ctl` script incluso nell' CloudWatch agente consente di specificare un file di configurazione, un parametro Parameter Store o la configurazione predefinita dell'agente. La configurazione predefinita si allinea al set di metriche di base predefinito e configura l'agente per riportare i parametri di memoria e spazio su disco. CloudWatch Tuttavia, non include alcuna configurazione dei file di registro. La configurazione predefinita viene applicata anche se si utilizza Systems Manager Quick Setup per l' CloudWatch agente.

Poiché la configurazione predefinita non include la registrazione e non è personalizzata in base alle esigenze dell'utente, si consiglia di creare e applicare CloudWatch configurazioni personalizzate, personalizzate in base alle proprie esigenze.

## Gestione delle configurazioni CloudWatch

Per impostazione predefinita, CloudWatch le configurazioni possono essere archiviate e applicate come parametri di Parameter Store o come CloudWatch file di configurazione. La scelta migliore dipenderà dalle vostre esigenze. In questa sezione, discutiamo i pro e i contro di queste due opzioni. Viene inoltre fornita una soluzione rappresentativa per la gestione dei file di CloudWatch configurazione per più account AWS e regioni AWS.

Parametri del Parameter Store di Systems Manager

L'utilizzo dei parametri Parameter Store per gestire CloudWatch le configurazioni funziona bene se disponi di un unico file di configurazione standard CloudWatch dell'agente che desideri applicare e gestire in un piccolo set di account e regioni AWS. Quando memorizzi le CloudWatch configurazioni come parametri di Parameter Store, puoi utilizzare lo strumento di configurazione dell' CloudWatch agente (`amazon-cloudwatch-agent-ctl`su Linux) per leggere e applicare la configurazione da Parameter Store senza dover copiare il file di configurazione sull'istanza. È possibile utilizzare il documento AmazonCloudWatch- ManageAgent  Systems Manager Command per aggiornare la CloudWatch configurazione su più istanze EC2 in un'unica esecuzione. Poiché i parametri di Parameter Store sono regionali, è necessario aggiornare e mantenere i CloudWatch parametri di Parameter Store in ogni regione AWS e account AWS. Se hai più CloudWatch configurazioni da applicare a ciascuna istanza, devi personalizzare il documento AmazonCloudWatch- ManageAgent Command per includere questi parametri.

CloudWatch file di configurazione

La gestione CloudWatch delle configurazioni come file potrebbe funzionare bene se disponi di molti account e regioni AWS e gestisci più file di CloudWatch configurazione. Utilizzando questo approccio, puoi sfogliarli, organizzarli e gestirli in una struttura di cartelle.  È possibile applicare regole di sicurezza a singole cartelle o file per limitare e concedere l'accesso, ad esempio autorizzazioni di aggiornamento e lettura. Puoi condividerli e trasferirli al di fuori di AWS per la collaborazione. Puoi controllare la versione dei file per tracciare e gestire le modifiche. È possibile applicare CloudWatch le configurazioni collettivamente copiando i file di configurazione nella directory di configurazione dell' CloudWatch agente senza applicare ogni file di configurazione singolarmente. Per Linux, la directory di CloudWatch configurazione si trova all'indirizzo. `/opt/aws/amazon-cloudwatch-agent/`

`etc/amazon-cloudwatch-agent.d` Per Windows, la directory di configurazione si trova in`C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs`.

Quando si avvia l' CloudWatch agente, l'agente aggiunge automaticamente ogni file trovato in queste directory per creare un file di configurazione CloudWatch composito. I file di configurazione devono essere archiviati in una posizione centrale (ad esempio, un bucket S3) a cui possono accedere gli account e le regioni richiesti. Viene fornito un esempio di soluzione che utilizza questo approccio.

Organizzazione delle CloudWatch configurazioni

Indipendentemente dall'approccio utilizzato per gestire le CloudWatch configurazioni, organizza le CloudWatch configurazioni. È possibile organizzare le configurazioni in percorsi di file o Parameter Store utilizzando un approccio come il seguente.

| | |
|---|---|
| /2 config/standard/windows/ec | Archivia file di CloudWatch configurazione standard specifici per Windows per Amazon EC2. Puoi classificare ulteriormente le configurazioni del sistema operativo (OS) standard per diverse versioni di Windows, tipi di istanze EC2 e ambienti in questa cartella. |
| /config/standard/windows/onpremises | Archivia i file di CloudWatch configurazione standard specifici di Windows per i server locali. In questa cartella puoi inoltre classific are ulteriormente le configurazioni del sistema operativo standard per diverse versioni di Windows, tipi di server e ambienti. |
| /2 config/standard/linux/ec | Archivia i tuoi file di CloudWatch configurazione standard specifici per Linux per Amazon EC2. Puoi classificare ulteriormente la configura zione del sistema operativo standard per diverse distribuzioni Linux, tipi di istanze EC2 e ambienti in questa cartella. |
| /config/standard/linux/onpremises | Archivia i tuoi file di configurazione standard specifici per Linux CloudWatch per i server locali. È possibile classificare ulteriormente la |

| | |
|---|---|
| | configurazione del sistema operativo standard per diverse distribuzioni Linux, tipi di server e ambienti in questa cartella. |
| /config/ecs | Archivia i file di CloudWatch configurazione specifici di Amazon Elastic Container Service (Amazon ECS) se utilizzi istanze di container Amazon ECS. Queste configurazioni possono essere aggiunte alle configurazioni standard di Amazon EC2 per la registrazione e il monitorag gio a livello di sistema specifici di Amazon ECS. |
| /config/ <application_name> | Archivia i file di configurazione specifici dell'appl icazione CloudWatch . È possibile classific are ulteriormente le applicazioni con cartelle e prefissi aggiuntivi per ambienti e versioni. |

## Esempio: memorizzazione dei file CloudWatch di configurazione in un bucket S3

Questa sezione fornisce un esempio di utilizzo di Amazon S3 per archiviare i file di CloudWatch configurazione e un runbook Systems Manager personalizzato per recuperare e applicare i file di configurazione. CloudWatch Questo approccio può risolvere alcune delle sfide legate all'utilizzo dei parametri di Systems Manager Parameter Store per la CloudWatch configurazione su larga scala:

- Se si utilizzano più regioni, è necessario sincronizzare gli aggiornamenti di CloudWatch configurazione nell'archivio dei parametri di ciascuna regione. Parameter Store è un servizio regionale e lo stesso parametro deve essere aggiornato in ogni regione che utilizza l' CloudWatch agente.
- Se si dispone di più CloudWatch configurazioni, è necessario avviare il recupero e l'applicazione di ciascuna configurazione di Parameter Store. È necessario recuperare singolarmente ogni CloudWatch configurazione dal Parameter Store e aggiornare anche il metodo di recupero ogni volta che si aggiunge una nuova configurazione. Al contrario, CloudWatch fornisce una directory di configurazione per l'archiviazione dei file di configurazione e applica ogni configurazione nella directory, senza richiedere che vengano specificate singolarmente.

- Se si utilizzano più account, è necessario assicurarsi che ogni nuovo account disponga CloudWatch delle configurazioni richieste nel relativo Parameter Store. È inoltre necessario assicurarsi che eventuali modifiche alla configurazione vengano applicate a questi account e alle relative regioni in futuro.

Puoi archiviare CloudWatch le configurazioni in un bucket S3 accessibile da tutti i tuoi account e regioni. È quindi possibile copiare queste configurazioni dal bucket S3 nella directory di CloudWatch configurazione utilizzando i runbook di Systems Manager Automation e Systems Manager State Manager. Puoi utilizzare il modello CloudFormation AWS cloudwatch-config-s3-bucket.yaml per creare un bucket S3 accessibile da più account all'interno di un'organizzazione in AWS Organizations. Il modello include un `OrganizationID` parametro che garantisce l'accesso in lettura a tutti gli account all'interno dell'organizzazione.

Il runbook di esempio aumentato di Systems Manager, fornito nella sezione Configurare State Manager and Distributor per la distribuzione e la configurazione degli CloudWatch agenti di questa guida, è configurato per recuperare i file utilizzando il bucket S3 creato dal modello AWS 3-bucket.yaml. cloudwatch-config-s CloudFormation

In alternativa, puoi utilizzare un sistema di controllo della versione (ad esempio) per archiviare i file di configurazione. GitHub Se desideri recuperare automaticamente i file di configurazione archiviati in un sistema di controllo delle versioni, devi gestire o centralizzare l'archiviazione delle credenziali e aggiornare il runbook di Systems Manager Automation utilizzato per recuperare le credenziali tra i tuoi account e. Regioni AWS

# Configurazione dell' CloudWatch agente per le istanze EC2 e i server locali

Molte organizzazioni eseguono carichi di lavoro sia su server fisici che su macchine virtuali (). VMs Questi carichi di lavoro vengono generalmente eseguiti su diversi OSs carichi di lavoro, ognuno con requisiti di installazione e configurazione unici per l'acquisizione e l'acquisizione delle metriche.

Se scegli di utilizzare le istanze EC2, puoi avere un elevato livello di controllo sulla configurazione dell'istanza e del sistema operativo. Tuttavia, questo livello più elevato di controllo e responsabilità richiede il monitoraggio e la regolazione delle configurazioni per ottenere un utilizzo più efficiente. È possibile migliorare l'efficacia operativa stabilendo standard per la registrazione e il monitoraggio e applicando un approccio di installazione e configurazione standard per l'acquisizione e l'acquisizione di log e metriche.

Organizations che migrano o estendono i propri investimenti IT al AWS cloud possono sfruttare CloudWatch per ottenere una soluzione di registrazione e monitoraggio unificata. CloudWatch il prezzo significa che paghi in modo incrementale per le metriche e i log che desideri acquisire. Puoi anche acquisire log e parametri per i server locali utilizzando un processo di installazione degli CloudWatch agenti simile a quello per Amazon EC2.

Prima di iniziare l'installazione e la distribuzione CloudWatch, assicurati di valutare le configurazioni di registrazione e metriche per i tuoi sistemi e le tue applicazioni. Assicurati di definire i log e le metriche standard che devi acquisire per quelli che desideri utilizzare. OSs I log e le metriche di sistema sono la base e lo standard per una soluzione di registrazione e monitoraggio perché sono generati dal sistema operativo e sono diversi per Linux e Windows. Esistono metriche e file di registro importanti disponibili in tutte le distribuzioni Linux, oltre a quelli specifici di una versione o distribuzione Linux. Questa varianza si verifica anche tra diverse versioni di Windows.

## Configurazione dell'agente CloudWatch

CloudWatch acquisisce parametri e log per Amazon EC2 e server locali utilizzando CloudWatch agenti e file di configurazione degli agenti specifici per ciascun sistema operativo. Ti consigliamo di definire i parametri standard della tua organizzazione e la configurazione di acquisizione dei log prima di iniziare a installare l' CloudWatch agente su larga scala nei tuoi account.

È possibile combinare più configurazioni di CloudWatch agenti per formare una configurazione composita CloudWatch dell'agente. Un approccio consigliato consiste nel definire e dividere le

configurazioni per i log e le metriche a livello di sistema e applicazione. Il diagramma seguente illustra come è possibile combinare più tipi di file di CloudWatch configurazione per requisiti diversi per formare una configurazione composita: CloudWatch

Questi log e metriche possono anche essere ulteriormente classificati e configurati per ambienti o requisiti specifici. Ad esempio, è possibile definire un sottoinsieme più piccolo di log e metriche con una precisione inferiore per gli ambienti di sviluppo non regolamentati e un set più ampio e completo con maggiore precisione per gli ambienti di produzione regolamentati.

## Configurazione dell'acquisizione dei log per le istanze EC2

Per impostazione predefinita, Amazon EC2 non monitora o acquisisce file di registro. Invece, i file di registro vengono acquisiti e inseriti nei CloudWatch registri dal software CloudWatch agente installato sull'istanza EC2, sull' AWS API o (). AWS Command Line Interface AWS CLI Consigliamo di utilizzare l' CloudWatch agente per importare i file di registro in CloudWatch Logs for Amazon EC2 e server locali.

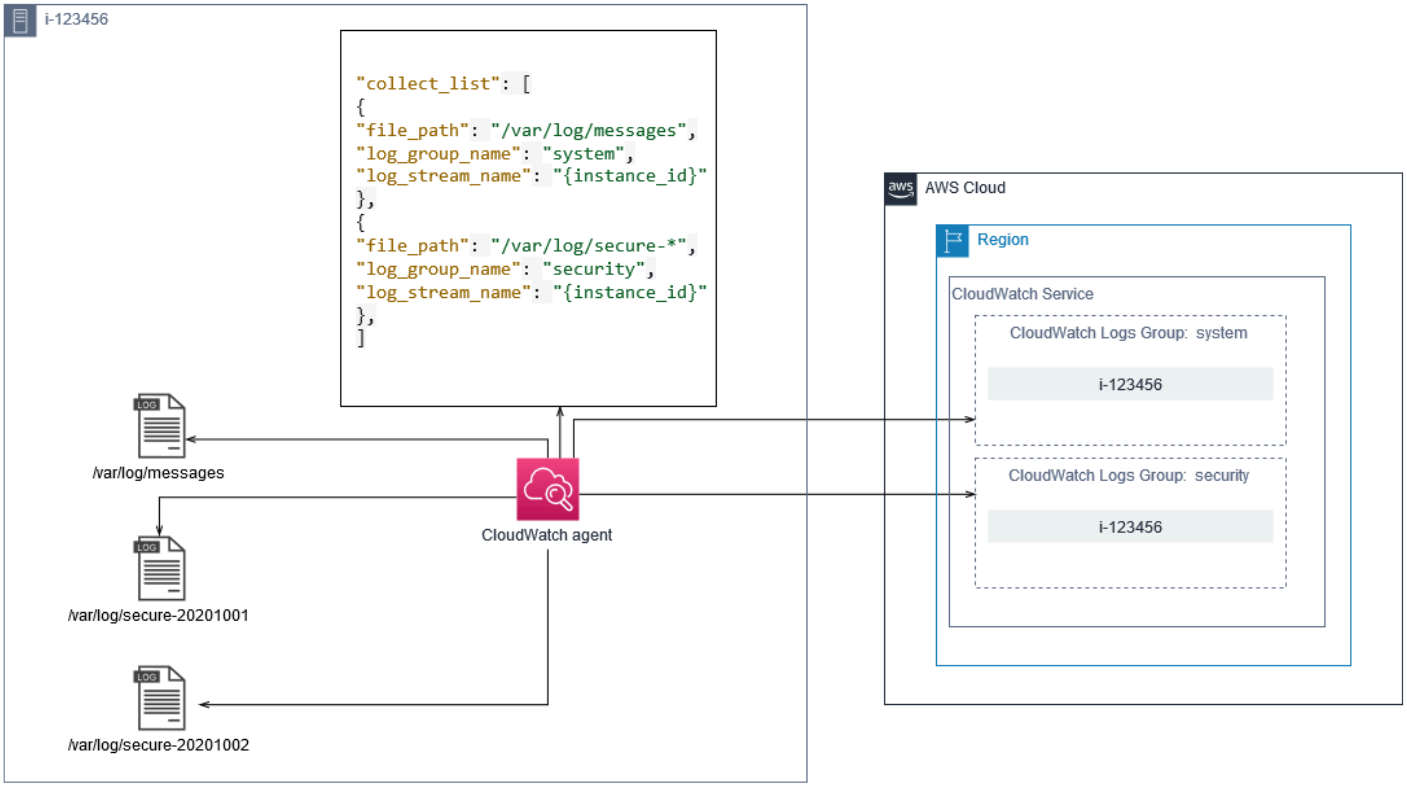
Puoi cercare e filtrare i log, nonché estrarre metriche ed eseguire l'automazione in base all'applicazione di patch di pattern dai file di registro. CloudWatch CloudWatch supporta opzioni di sintassi di filtro e pattern in formato testo semplice, delimitato da spazi e in formato JSON, con log in formato JSON che offrono la massima flessibilità. Per aumentare le opzioni di filtraggio e analisi, è necessario utilizzare un output di registro formattato anziché testo semplice.

L' CloudWatch agente utilizza un file di configurazione che definisce i log e le metriche a cui inviare. CloudWatch CloudWatch quindi acquisisce ogni file di registro come flusso di log e raggruppa questi flussi di log in un gruppo di log. Questo ti aiuta a eseguire operazioni tra i log delle tue istanze EC2, come la ricerca di una stringa corrispondente.

Il nome del flusso di log predefinito è lo stesso dell'ID dell'istanza EC2 e il nome del gruppo di log predefinito è lo stesso del percorso del file di registro. Il nome del flusso di log deve essere univoco all'interno del gruppo di CloudWatch log. È possibile utilizzare`instance_id`, `hostnamelocal_hostname`, o `ip_address` per la sostituzione dinamica nei nomi dei flussi di log e dei gruppi di log, il che significa che è possibile utilizzare lo stesso file di configurazione dell' CloudWatch agente su più istanze EC2.

Il diagramma seguente mostra una configurazione dell' CloudWatch agente per l'acquisizione dei log. Il gruppo di log è definito dai file di registro acquisiti e contiene flussi di log separati per ogni istanza

EC2, poiché la `{instance_id}` variabile viene utilizzata per il nome del flusso di log e l'istanza EC2 è unica. IDs




I gruppi di log definiscono la conservazione, i tag, la sicurezza, i filtri metrici e l'ambito di ricerca per i flussi di log che contengono. Il comportamento di raggruppamento predefinito basato sul nome del file di registro consente di cercare, creare metriche e avvisi sui dati specifici di un file di registro tra le istanze EC2 di un account e di una regione. È necessario valutare se è necessario un ulteriore perfezionamento del gruppo di log. Ad esempio, il tuo account potrebbe essere condiviso da più unità aziendali e avere titolari tecnici o operativi diversi. Ciò significa che è necessario rifinire ulteriormente il nome del gruppo di log per riflettere la separazione e la proprietà. Questo approccio consente di concentrare l'analisi e la risoluzione dei problemi sull'istanza EC2 pertinente.

Se più ambienti utilizzano un account, puoi separare la registrazione per i carichi di lavoro eseguiti in ogni ambiente. La tabella seguente mostra una convenzione di denominazione dei gruppi di log che include l'unità di business, il progetto o l'applicazione e l'ambiente.

| | |
|---|---|
| Nome del gruppo di log | `/<Business unit>/<Project or application name>/<Environment>/<Log file name>` |

| | |
|---|---|
| Nome del flusso di registro | `<EC2 instance ID>` |

Puoi anche raggruppare tutti i file di registro di un'istanza EC2 nello stesso gruppo di log. Ciò semplifica la ricerca e l'analisi su un set di file di registro per una singola istanza EC2. Ciò è utile se la maggior parte delle istanze EC2 serve un'applicazione o un carico di lavoro e ogni istanza EC2 ha uno scopo specifico. La tabella seguente mostra come il gruppo di log e la denominazione dei flussi di log potrebbero essere formattati per supportare questo approccio.

| | |
|---|---|
| Nome del gruppo di log | `/<Business unit>/<Project or application name>/<Environment>/<EC2 instance ID>` |
| Nome del flusso di registro | `<Log file name>` |

## Configurazione dell'acquisizione delle metriche per le istanze EC2

Per impostazione predefinita, le istanze EC2 sono abilitate per il monitoraggio di base e un set standard di parametri (ad esempio, parametri relativi alla CPU, alla rete o allo storage) viene inviato automaticamente ogni cinque minuti. CloudWatch CloudWatch le metriche possono variare a seconda della famiglia di istanze, ad esempio, le istanze con prestazioni espandibili dispongono di metriche per i crediti CPU. I parametri standard di Amazon EC2 sono inclusi nel prezzo dell'istanza. Se abiliti il monitoraggio dettagliato per le tue istanze EC2, puoi ricevere dati in periodi di un minuto. La frequenza dei periodi influisce sui CloudWatch costi, quindi assicurati di valutare se è necessario un monitoraggio dettagliato per tutte le istanze EC2 o solo per alcune. Ad esempio, puoi abilitare il monitoraggio dettagliato per i carichi di lavoro di produzione ma utilizzare il monitoraggio di base per i carichi di lavoro non di produzione.

I server locali non includono alcuna metrica predefinita CloudWatch e devono utilizzare l' CloudWatch agente o AWS l'SDK per acquisire le metriche. AWS CLI Ciò significa che è necessario definire le metriche che si desidera acquisire (ad esempio, l'utilizzo della CPU) nel file di configurazione. CloudWatch Puoi creare un file di CloudWatch configurazione unico che includa i parametri standard delle istanze EC2 per i tuoi server locali e applicarlo in aggiunta alla configurazione standard. CloudWatch

Le metriche in CloudWatch sono definite in modo univoco dal nome della metrica e da zero o più dimensioni e sono raggruppate in modo univoco in uno spazio dei nomi metrico. Le metriche fornite da un AWS servizio hanno uno spazio dei nomi che inizia con `AWS` (ad esempio) e le metriche non metriche sono considerate metriche personalizzate. `AWS/EC2`AWS Le metriche configurate e acquisite con l' CloudWatch agente sono tutte considerate metriche personalizzate. Poiché il numero di metriche create influisce sui CloudWatch costi, è necessario valutare se ciascuna metrica è necessaria per tutte o solo alcune delle istanze EC2. Ad esempio, è possibile definire un set completo di metriche per i carichi di lavoro di produzione, ma utilizzare un sottoinsieme più piccolo di tali metriche per i carichi di lavoro non di produzione.

`CWAgent`è lo spazio dei nomi predefinito per le metriche pubblicate dall'agente. CloudWatch Analogamente ai gruppi di log, lo spazio dei nomi delle metriche organizza un set di metriche in modo che possano essere trovate insieme in un unico posto. È necessario modificare lo spazio dei nomi in modo che rifletta un'unità aziendale, un progetto o un'applicazione e un ambiente (ad esempio,). `/<Business unit>/<Project or application name>/<Environment>` Questo approccio è utile se più carichi di lavoro non correlati utilizzano lo stesso account. È inoltre possibile correlare la convenzione di denominazione dei namespace alla convenzione di denominazione dei gruppi di log. CloudWatch

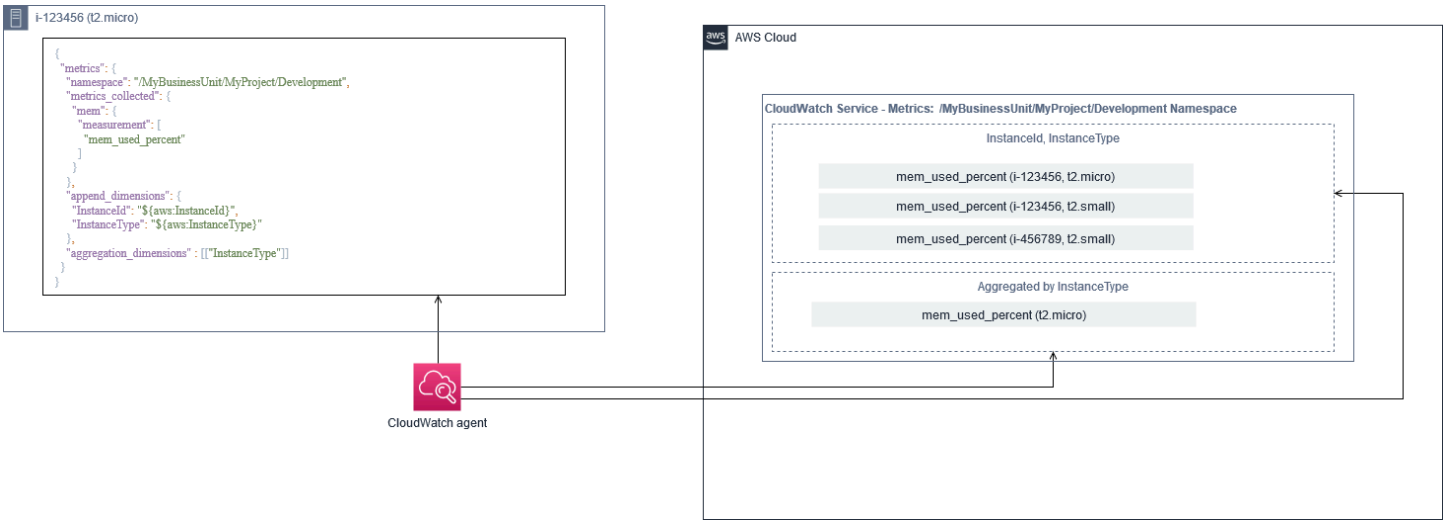
Le metriche sono identificate anche in base alle loro dimensioni, che aiutano ad analizzarle rispetto a una serie di condizioni e sono le proprietà in base alle quali vengono registrate le osservazioni. Amazon EC2 include parametri separati per le istanze EC2 con e dimensioni. `InstanceId` `AutoScalingGroupName` Se abiliti il monitoraggio dettagliato, ricevi anche metriche con le `InstanceType` dimensioni `ImageId` e. Ad esempio, Amazon EC2 fornisce una metrica di istanza EC2 separata per l'utilizzo della CPU con le `InstanceId` dimensioni, oltre a una metrica di utilizzo della CPU separata per la dimensione. `InstanceType` Questo ti aiuta ad analizzare l'utilizzo della CPU per ogni istanza EC2 unica, oltre a tutte le istanze EC2 di un tipo di istanza specifico.

L'aggiunta di altre dimensioni aumenta la capacità di analisi ma aumenta anche i costi complessivi, poiché ogni combinazione di metrica e valore di dimensione univoca si traduce in una nuova metrica. Ad esempio, se si crea una metrica per la percentuale di utilizzo della memoria rispetto alla `InstanceId` dimensione, si tratta di una nuova metrica per ogni istanza EC2. Se la tua organizzazione gestisce migliaia di istanze EC2, ciò comporta migliaia di metriche e comporta costi più elevati. Per controllare e prevedere i costi, assicurati di determinare la cardinalità della metrica e quali dimensioni aggiungono il maggior valore. Ad esempio, puoi definire un set completo di dimensioni per le metriche del carico di lavoro di produzione, ma un sottoinsieme più piccolo di queste dimensioni per i carichi di lavoro non di produzione.

È possibile utilizzare la `append_dimensions` proprietà per aggiungere dimensioni a una o tutte le metriche definite nella configurazione. CloudWatch Puoi anche aggiungere dinamicamente`ImageId`, `InstanceIdInstanceType`, e `AutoScalingGroupName` a tutte le metriche della tua configurazione. CloudWatch In alternativa, puoi aggiungere un nome e un valore di dimensione arbitrari per metriche specifiche utilizzando la proprietà relativa a quella metrica. `append_dimensions` CloudWatch può anche aggregare le statistiche sulle dimensioni metriche definite con la proprietà. `aggregation_dimensions`

Ad esempio, è possibile aggregare la memoria utilizzata rispetto alla `InstanceType` dimensione per visualizzare la memoria media utilizzata da tutte le istanze EC2 per ogni tipo di istanza. Se utilizzi `t2.micro` istanze in esecuzione in una regione, puoi determinare se i carichi di lavoro che utilizzano la `t2.micro` classe stanno utilizzando eccessivamente o sottoutilizzando la memoria fornita. Il sottoutilizzo potrebbe essere un segno di carichi di lavoro che utilizzano classi EC2 con una capacità di memoria non richiesta. Al contrario, l'utilizzo eccessivo potrebbe essere un segno di carichi di lavoro che utilizzano classi Amazon EC2 con memoria insufficiente.

Il diagramma seguente mostra un esempio di configurazione dei CloudWatch parametri che utilizza uno spazio dei nomi personalizzato, dimensioni aggiunte e aggregazione per. `InstanceType`




# Configurazione a livello di sistema CloudWatch

Le metriche e i log a livello di sistema sono un componente centrale di una soluzione di monitoraggio e registrazione e l' CloudWatch agente dispone di opzioni di configurazione specifiche per Windows e Linux.

Si consiglia di utilizzare la procedura guidata del file di CloudWatch configurazione o lo schema del file di configurazione per definire il file di configurazione dell' CloudWatch agente per ogni sistema operativo che si intende supportare. È possibile definire log e metriche aggiuntivi a livello di sistema operativo specifici del carico di lavoro in file di configurazione separati CloudWatch e aggiunti alla configurazione standard. Questi file di configurazione unici devono essere archiviati separatamente in un bucket S3 dove possono essere recuperati dalle istanze EC2. Un esempio di configurazione di un bucket S3 per questo scopo è descritto nella sezione di questa guida. Gestione delle configurazioni CloudWatch È possibile recuperare e applicare automaticamente queste configurazioni utilizzando State Manager and Distributor.

## Configurazione dei log a livello di sistema

I log a livello di sistema sono essenziali per la diagnosi e la risoluzione dei problemi in locale o sul cloud. AWS L'approccio utilizzato per l'acquisizione dei log dovrebbe includere tutti i log di sistema e di sicurezza generati dal sistema operativo. I file di registro generati dal sistema operativo potrebbero essere diversi a seconda della versione del sistema operativo.

L' CloudWatch agente supporta il monitoraggio dei registri degli eventi di Windows fornendo il nome del registro eventi. È possibile scegliere quali registri eventi di Windows monitorare (ad esempio `SystemApplication`, o`Security`).

I registri di sistema, delle applicazioni e di sicurezza per i sistemi Linux sono in genere archiviati nella `/var/log` directory. La tabella seguente definisce i file di registro predefiniti comuni da monitorare, ma è necessario controllare il `/etc/syslog.conf` file `/etc/rsyslog.conf` o per determinare la configurazione specifica per i file di registro del sistema.

| | |
|---|---|
| Distribuzione Fedora | `/var/log/boot.log*` — Registro di avvio |
| (Amazon Linux, CentOS, Red Hat Enterprise Linux) | `/var/log/dmesg` — Registro del kernel |
| | `/var/log/secure` — Registro di sicurezza e autenticazione |
| | `/var/log/messages` — Registro generale di sistema |
| | `/var/log/cron*` — Cron Logs |

| | | |
|---|---|---|
| | | `/var/log/cloud-init-output.log` — Uscita da script di avvio `Userdata` |
| Debian<br><br>(Ubuntu) | | `/var/log/syslog` — Registro di avvio |
| | | `/var/log/cloud-init-output.log` — Output dagli script di `Userdata` avvio |
| | | `/var/log/auth.log` — Registro di sicurezza e autenticazione |
| | | `/var/log/kern.log` — Registro del kernel |

L'organizzazione potrebbe disporre anche di altri agenti o componenti di sistema che generano log da monitorare. È necessario valutare e decidere quali file di registro vengono generati da questi agenti o applicazioni e includerli nella configurazione identificando la posizione dei file. Ad esempio, è necessario includere i registri di Systems Manager e degli CloudWatch agenti nella configurazione. La tabella seguente fornisce la posizione di questi registri degli agenti per Windows e Linux.

| | | |
|---|---|---|
| Windows | CloudWatch agente | `$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log` |
| | Agente Systems Manager | `%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log`<br><br>`%PROGRAMDATA%\Amazon\SSM\Logs\errors.log`<br><br>`%PROGRAMDATA%\Amazon\SSM\Logs\audits\amazon-ssm-agent-audit-YYYY-MM-DD` |

| | | |
|---|---|---|
| Linux | CloudWatch agente | `/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log` |
| | Agente Systems Manager | `/var/log/amazon/ssm/amazon-ssm-agent.log`<br>`/var/log/amazon/ssm/errors.log`<br>`/var/log/amazon/ssm/audits/amazon-ssm-agent-audit-YYYY-MM-DD` |

CloudWatch ignora un file di registro se il file di registro è definito nella configurazione dell' CloudWatch agente ma non viene trovato. Ciò è utile quando si desidera mantenere una singola configurazione di registro per Linux, anziché configurazioni separate per ogni distribuzione. È utile anche quando un file di registro non esiste finché l'agente o l'applicazione software non inizia a funzionare.

## Configurazione delle metriche a livello di sistema

L'utilizzo della memoria e dello spazio su disco non è incluso nei parametri standard forniti da Amazon EC2. Per includere questi parametri, devi installare e configurare l' CloudWatch agente sulle tue istanze EC2. La procedura guidata di configurazione dell' CloudWatch agente crea una CloudWatch configurazione con metriche predefinite e puoi aggiungere o rimuovere metriche secondo necessità. Assicurati di rivedere i set di metriche predefiniti per determinare il livello appropriato richiesto.

Gli utenti finali e i proprietari dei carichi di lavoro devono pubblicare parametri di sistema aggiuntivi in base a requisiti specifici per un server o un'istanza EC2. Queste definizioni delle metriche devono essere archiviate, versionate e gestite in un file di configurazione CloudWatch dell'agente separato e condivise in una posizione centrale (ad esempio, Amazon S3) per il riutilizzo e l'automazione.

I parametri standard di Amazon EC2 non vengono acquisiti automaticamente nei server locali. Queste metriche devono essere definite in un file di configurazione CloudWatch dell'agente utilizzato dalle istanze locali. È possibile creare un file di configurazione delle metriche separato per le istanze locali con metriche come l'utilizzo della CPU e aggiungere queste metriche al file di configurazione delle metriche standard.

# Configurazione a livello di applicazione CloudWatch

I log e le metriche delle applicazioni vengono generati dalle applicazioni in esecuzione e sono specifici dell'applicazione. Assicuratevi di definire i log e le metriche necessari per monitorare adeguatamente le applicazioni che vengono utilizzate regolarmente dall'organizzazione. Ad esempio, l'organizzazione potrebbe aver adottato come standard Microsoft Internet Information Server (IIS) per le applicazioni basate sul Web. È possibile creare una CloudWatch configurazione standard di log e metrica per IIS che può essere utilizzata anche in tutta l'organizzazione. I file di configurazione specifici dell'applicazione possono essere archiviati in una posizione centralizzata (ad esempio, un bucket S3) e sono accessibili dai proprietari dei carichi di lavoro o tramite recupero automatico e copiati nella directory di configurazione. CloudWatch L' CloudWatch agente combina automaticamente i file di CloudWatch configurazione presenti nella directory dei file di configurazione di ogni istanza o server EC2 in una configurazione composita. CloudWatch Il risultato finale è una CloudWatch configurazione che include la configurazione standard a livello di sistema dell'organizzazione, oltre a tutte le configurazioni pertinenti a livello di applicazione. CloudWatch

I proprietari dei carichi di lavoro devono identificare e configurare i file di registro e le metriche per tutte le applicazioni e i componenti critici.

## Configurazione dei log a livello di applicazione

La registrazione a livello di applicazione varia a seconda che l'applicazione sia un'applicazione commerciale (COTS) o sviluppata su misura. off-the-shelf Le applicazioni COTS e i relativi componenti possono fornire diverse opzioni per la configurazione e l'output dei registri, come il livello di dettaglio del registro, il formato dei file di registro e la posizione dei file di registro. Tuttavia, la maggior parte delle applicazioni COTS o di terze parti non consente di modificare radicalmente la registrazione (ad esempio, l'aggiornamento del codice dell'applicazione per includere istruzioni di registro aggiuntive o formati non configurabili). Come minimo, è necessario configurare le opzioni di registrazione per COTS o applicazioni di terze parti per registrare avvisi e informazioni a livello di errore, preferibilmente in formato JSON.

È possibile integrare applicazioni sviluppate su misura con CloudWatch Logs includendo i file di registro dell'applicazione nella configurazione. CloudWatch Le applicazioni personalizzate offrono una migliore qualità e controllo dei log perché consentono di personalizzare il formato di output dei log, classificare e separare l'output dei componenti in file di registro separati, oltre a includere eventuali dettagli aggiuntivi richiesti. Assicurati di rivedere e standardizzare le librerie di registrazione e i dati e la formattazione richiesti per la tua organizzazione, in modo da semplificare l'analisi e l'elaborazione.

Puoi anche scrivere su un flusso di CloudWatch log con la chiamata `PutLogEvents` API CloudWatch Logs o utilizzando l'SDK. AWS Puoi utilizzare l'API o l'SDK per requisiti di registrazione personalizzati, come coordinare la registrazione su un singolo flusso di log su un set distribuito di componenti e server. Tuttavia, la soluzione più semplice da gestire e più ampiamente applicabile consiste nel configurare le applicazioni per la scrittura nei file di registro e quindi utilizzare l' CloudWatch agente per leggere e trasmettere i file di registro. CloudWatch

È inoltre necessario considerare il tipo di metriche che si desidera misurare dai file di registro delle applicazioni. È possibile utilizzare i filtri metrici per misurare, rappresentare graficamente e generare allarmi in base a questi dati in un gruppo di CloudWatch log. Ad esempio, puoi utilizzare un filtro metrico per contare i tentativi di accesso non riusciti identificandoli nei log.

È inoltre possibile creare metriche personalizzate per le applicazioni sviluppate su misura utilizzando il formato metrico CloudWatch incorporato nei file di registro dell'applicazione.

## Configurazione delle metriche a livello di applicazione

Le metriche personalizzate sono metriche che non vengono fornite direttamente dai AWS servizi a CloudWatch e sono pubblicate in un namespace personalizzato all'interno delle metriche. CloudWatch Tutte le metriche delle applicazioni sono considerate metriche personalizzate. CloudWatch Le metriche delle applicazioni potrebbero essere allineate a un'istanza EC2, a un componente dell'applicazione, a una chiamata API o persino a una funzione aziendale. È inoltre necessario considerare l'importanza e la cardinalità delle dimensioni scelte per le metriche. Le dimensioni con cardinalità elevata generano un gran numero di metriche personalizzate e potrebbero aumentare i costi. CloudWatch

CloudWatch consente di acquisire metriche a livello di applicazione in diversi modi, tra cui:

- Acquisisci metriche a livello di processo definendo i singoli processi che desideri acquisire dal plug-in procstat.

- Un'applicazione pubblica una metrica su Windows Performance Monitor e questa metrica viene definita nella configurazione. CloudWatch
- I filtri e i pattern metrici vengono applicati ai log in di un'applicazione. CloudWatch
- Un'applicazione scrive su un CloudWatch registro utilizzando il formato metrico CloudWatch incorporato.
- Un'applicazione invia una metrica CloudWatch tramite l'API o AWS l'SDK.
- Un'applicazione invia una metrica a un demone collectd o StatsD con un agente configurato. CloudWatch

È possibile utilizzare procstat per monitorare e misurare i processi applicativi critici con l'agente. CloudWatch Ciò consente di generare un allarme e agire (ad esempio, una notifica o un processo di riavvio) se un processo critico non è più in esecuzione per l'applicazione. È inoltre possibile misurare le caratteristiche prestazionali dei processi applicativi e generare un allarme se un particolare processo si comporta in modo anomalo.

Il monitoraggio di Procstat è utile anche se non è possibile aggiornare le applicazioni COTS con metriche personalizzate aggiuntive. Ad esempio, puoi creare una `my_process` metrica che misuri `cpu_time` e includa una dimensione personalizzata. `application_version` Puoi anche utilizzare più file di configurazione CloudWatch dell'agente per un'applicazione se hai dimensioni diverse per metriche diverse.

Se l'applicazione viene eseguita su Windows, è necessario valutare se pubblica già le metriche su Windows Performance Monitor. Molte applicazioni COTS si integrano con Windows Performance Monitor, il che consente di monitorare facilmente le metriche delle applicazioni. CloudWatch si integra anche con Windows Performance Monitor ed è possibile acquisire tutte le metriche già disponibili al suo interno.

Assicurati di esaminare il formato di registrazione e le informazioni di registro fornite dalle applicazioni per determinare quali metriche possono essere estratte con i filtri metrici. È possibile esaminare i log cronologici dell'applicazione per determinare come vengono rappresentati i messaggi di errore e gli arresti anomali. È inoltre necessario esaminare i problemi segnalati in precedenza per determinare se è possibile acquisire una metrica per evitare che il problema si ripresenti. È inoltre necessario consultare la documentazione dell'applicazione e chiedere agli sviluppatori dell'applicazione di confermare in che modo è possibile identificare i messaggi di errore.

Per le applicazioni sviluppate su misura, collaborate con gli sviluppatori dell'applicazione per definire metriche importanti che possono essere implementate utilizzando il formato metrico CloudWatch

incorporato, l' AWS SDK o l'API. AWS L'approccio consigliato consiste nell'utilizzare il formato metrico incorporato. Puoi utilizzare le librerie di formati metrici incorporati open source AWS fornite per aiutarti a scrivere le tue dichiarazioni nel formato richiesto. È inoltre necessario aggiornare la CloudWatch configurazione specifica dell'applicazione per includere l'agente di formato metrico incorporato. Ciò fa sì che l'agente in esecuzione sull'istanza EC2 agisca come un endpoint locale in formato metrico incorporato che invia metriche in formato metrico incorporato a. CloudWatch

Se le tue applicazioni supportano già le metriche di pubblicazione su collectd o statsd, puoi sfruttarle per importare le metriche. CloudWatch

# CloudWatch approcci di installazione di agenti per Amazon EC2 e server locali

L'automazione del processo di installazione dell' CloudWatch agente consente di distribuirlo in modo rapido e coerente e di acquisire i log e i parametri richiesti. Esistono diversi approcci per automatizzare l'installazione dell' CloudWatch agente, incluso il supporto per più account e più regioni. Vengono discussi i seguenti approcci di installazione automatizzata:

- Installazione dell' CloudWatch agente utilizzando Systems Manager Distributor e Systems Manager State Manager: consigliamo di utilizzare questo approccio se le istanze EC2 e i server locali eseguono l'agente Systems Manager. Ciò garantisce che l' CloudWatch agente sia sempre aggiornato e che sia possibile creare report e risolvere i problemi sui server che non dispongono dell'agente. CloudWatch Questo approccio è inoltre scalabile per supportare più account e regioni.
- Implementazione dell' CloudWatch agente come parte dello script dei dati utente durante il provisioning dell'istanza EC2: Amazon EC2 consente di definire uno script di avvio che viene eseguito al primo avvio o riavvio. Puoi definire uno script per automatizzare il processo di download e installazione dell'agente. Questo può essere incluso anche negli CloudFormation script e nei prodotti AWS Service Catalog. Questo approccio può essere appropriato in base alle esigenze se esiste un approccio personalizzato all'installazione e alla configurazione degli agenti per un carico di lavoro specifico che si discosta dagli standard.
- Inclusione dell' CloudWatchagente in Amazon Machine Images (AMIs): puoi installare l' CloudWatchagente nelle tue AMI personalizzate per Amazon EC2. L'agente verrà installato e avviato automaticamente sulle istanze EC2 che utilizzano l'AMI. Tuttavia, è necessario assicurarsi che l'agente e la sua configurazione vengano aggiornati regolarmente.

## Installazione dell' CloudWatch agente utilizzando Systems Manager Distributor e State Manager

È possibile utilizzare Systems Manager State Manager con Systems Manager Distributor per installare e aggiornare automaticamente l' CloudWatch agente su server e istanze EC2. Distributor include il pacchetto `AmazonCloudWatchAgent` AWS gestito che installa la versione dell'agente più recente. CloudWatch

Questo approccio di installazione presenta i seguenti prerequisiti:

- L'agente Systems Manager deve essere installato e in esecuzione sui server o sulle istanze EC2. L'agente Systems Manager è preinstallato su Amazon Linux, Amazon Linux 2 e altri AMIs. L'agente deve inoltre essere installato e configurato su altre immagini o in locale VMs e sui server.

> **Note**
>
> Amazon Linux 2 sta per terminare il supporto. Per ulteriori informazioni, consulta Amazon Linux 2 FAQs.

- Un ruolo o delle credenziali IAM con le autorizzazioni richieste CloudWatch e Systems Manager devono essere collegati all'istanza EC2 o definiti nel file delle credenziali per un server locale. Ad esempio, puoi creare un ruolo IAM che includa le policy AWS gestite: `AmazonSSMManagedInstanceCore` per Systems Manager e `CloudWatchAgentServerPolicy` for CloudWatch. Puoi utilizzare il CloudFormation template ssm-cloudwatch-instance-role.yaml per distribuire un ruolo e un profilo di istanza IAM che includa entrambe queste policy. Questo modello può anche essere modificato per includere altre autorizzazioni IAM standard per le istanze EC2. Per i server locali o VMs, deve configurare l' CloudWatch agente per utilizzare il ruolo del servizio Systems Manager configurato per il server locale. Per ulteriori informazioni su questo argomento, vedi Come posso configurare i server locali che utilizzano Systems Manager Agent e l'agente unificato per utilizzare solo CloudWatch credenziali temporanee? nel Knowledge Center. AWS

L'elenco seguente offre diversi vantaggi per l'utilizzo dell'approccio Systems Manager Distributor e State Manager per l'installazione e la manutenzione dell' CloudWatch agente:

- Installazione automatizzata per più sistemi OSs: non è necessario scrivere e gestire uno script per ogni sistema operativo per scaricare e installare l' CloudWatchagente.
- Controlli automatici degli aggiornamenti: State Manager verifica automaticamente e regolarmente che ogni istanza EC2 disponga della CloudWatch versione più recente.
- Reporting sulla conformità: la dashboard di conformità di Systems Manager mostra quali istanze EC2 non sono riuscite a installare correttamente il pacchetto Distributor.
- Installazione automatizzata per le istanze EC2 appena lanciate: le nuove istanze EC2 che vengono avviate sull'account ricevono automaticamente l'agente. CloudWatch

Tuttavia, dovresti considerare anche le seguenti tre aree prima di scegliere questo approccio:

- Collisione con un'associazione esistente: se un'altra associazione installa o configura già l' CloudWatch agente, le due associazioni potrebbero interferire tra loro e potenzialmente causare problemi. Quando si utilizza questo approccio, è necessario rimuovere tutte le associazioni esistenti che installano o aggiornano l' CloudWatchagente e la configurazione.
- Aggiornamento dei file di configurazione personalizzati dell'agente: Distributor esegue un'installazione utilizzando il file di configurazione predefinito. Se si utilizza un file di configurazione personalizzato o più file di CloudWatch configurazione, è necessario aggiornare la configurazione dopo l'installazione.
- Configurazione multiregionale o multiaccount: l'associazione State Manager deve essere configurata in ogni account e regione. I nuovi account in un ambiente con più account devono essere aggiornati per includere l'associazione State Manager. È necessario centralizzare o sincronizzare la CloudWatch configurazione in modo che più account e regioni possano recuperare e applicare gli standard richiesti.

## Configura State Manager and Distributor per CloudWatch la distribuzione e la configurazione degli agenti

È possibile utilizzare Systems Manager Quick Setup per configurare rapidamente le funzionalità di Systems Manager, tra cui l'installazione e l'aggiornamento automatici dell' CloudWatch agente sulle istanze EC2. Il Quick Setup implementa uno CloudFormation stack che distribuisce e configura le risorse di Systems Manager in base alle scelte dell'utente.

L'elenco seguente fornisce due azioni importanti che vengono eseguite da Quick Setup per l'installazione e l'aggiornamento automatici degli CloudWatch agenti:

1. Creazione di documenti personalizzati di Systems Manager: Quick Setup crea i seguenti documenti di Systems Manager da utilizzare con State Manager. I nomi dei documenti possono variare ma il contenuto rimane lo stesso:
   - `CreateAndAttachIAMToInstance`— Crea il `AmazonSSMRoleForInstancesQuickSetup` ruolo e il profilo dell'istanza se non esistono e associa la `AmazonSSMManagedInstanceCore` policy al ruolo. Ciò non include la policy `CloudWatchAgentServerPolicy` IAM richiesta. È necessario aggiornare questa politica e aggiornare questo documento Systems Manager per includerla come descritto nella sezione seguente.

- `InstallAndManageCloudWatchDocument`— Installa l' CloudWatch agente con Distributor e configura ogni istanza EC2 una volta con una configurazione CloudWatch agente predefinita utilizzando il documento Systems Manager`AWS-ConfigureAWSPackage`.
- `UpdateCloudWatchDocument`— Aggiorna l' CloudWatch agente installando l' CloudWatch agente più recente utilizzando il documento `AWS-ConfigureAWSPackage` Systems Manager. L'aggiornamento o la disinstallazione dell'agente non rimuove i file di CloudWatch configurazione esistenti dall'istanza EC2.

2. Crea associazioni State Manager: le associazioni State Manager vengono create e configurate per utilizzare i documenti Systems Manager creati su misura. I nomi delle associazioni di State Manager possono variare ma la configurazione rimane la stessa:
   - `ManageCloudWatchAgent`— Esegue il documento `InstallAndManageCloudWatchDocument` Systems Manager una volta per ogni istanza EC2.
   - `UpdateCloudWatchAgent`— Esegue il documento `UpdateCloudWatchDocument` Systems Manager ogni 30 giorni per ogni istanza EC2.
   - Esegue il documento `CreateAndAttachIAMToInstance` Systems Manager una volta per ogni istanza EC2.

È necessario aumentare e personalizzare la configurazione Quick Setup completata per includere CloudWatch le autorizzazioni e supportare configurazioni personalizzate. CloudWatch In particolare, sarà necessario `CreateAndAttachIAMToInstance` aggiornare il `InstallAndManageCloudWatchDocument` documento e il documento. È possibile aggiornare manualmente i documenti Systems Manager creati da Quick Setup. In alternativa, è possibile utilizzare il proprio CloudFormation modello per fornire alle stesse risorse gli aggiornamenti necessari, nonché configurare e distribuire altre risorse Systems Manager e non utilizzare Quick Setup.

> **Important**
>
> Quick Setup crea uno CloudFormation stack per distribuire e configurare le risorse di Systems Manager in base alle tue scelte. Se si aggiornano le opzioni di configurazione rapida, potrebbe essere necessario riaggiornare manualmente i documenti di Systems Manager.

Le sezioni seguenti descrivono come aggiornare manualmente le risorse di Systems Manager create da Quick Setup, nonché come utilizzare il proprio CloudFormation modello per eseguire una configurazione rapida aggiornata. Si consiglia di utilizzare un CloudFormation modello personalizzato per evitare di aggiornare manualmente le risorse create da Quick Setup e CloudFormation.

## Usa Systems Manager Quick Setup e aggiorna manualmente le risorse Systems Manager create

Le risorse Systems Manager create con l'approccio Quick Setup devono essere aggiornate per includere le autorizzazioni degli CloudWatch agenti richieste e supportare più file di CloudWatch configurazione. Questa sezione descrive come aggiornare il ruolo IAM e i documenti Systems Manager per utilizzare un bucket S3 centralizzato contenente CloudWatch configurazioni accessibili da più account. La creazione di un bucket S3 per archiviare i file di CloudWatch configurazione è descritta nella sezione di questa guida. Gestione delle configurazioni CloudWatch

### Aggiornare il documento **`CreateAndAttachIAMToInstance`** Systems Manager

Questo documento Systems Manager creato da Quick Setup verifica se a un'istanza EC2 è associato un profilo di istanza IAM esistente. In caso affermativo, associa la `AmazonSSMManagedInstanceCore` policy al ruolo esistente. Ciò protegge le istanze EC2 esistenti dalla perdita delle AWS autorizzazioni che potrebbero essere assegnate tramite i profili di istanza esistenti. È necessario aggiungere un passaggio in questo documento per allegare la policy `CloudWatchAgentServerPolicy` IAM alle istanze EC2 a cui è già associato un profilo di istanza. Il documento Systems Manager crea anche il ruolo IAM se non esiste e a un'istanza EC2 non è associato un profilo di istanza. È necessario aggiornare questa sezione del documento per includere anche la policy `CloudWatchAgentServerPolicy` IAM.

Esamina il documento di esempio CreateAndAttachIAMToInstance.yaml completato e confrontalo con il documento creato da Quick Setup. Modifica il documento esistente per includere i passaggi e le modifiche richiesti. In base alle scelte di configurazione rapida, il documento creato da Quick Setup potrebbe essere diverso dal documento di esempio fornito, pertanto assicuratevi di apportare le modifiche necessarie. Il documento di esempio include la scelta dell'opzione Quick Setup per la scansione quotidiana delle istanze alla ricerca di patch mancanti e include quindi una policy per Systems Manager Patch Manager.

### Aggiornare il documento **`InstallAndManageCloudWatchDocument`** Systems Manager

Questo documento Systems Manager creato da Quick Setup installa l' CloudWatch agente e lo configura con la configurazione dell' CloudWatch agente predefinita. La CloudWatch configurazione predefinita si allinea al set di metriche di base predefinito. È necessario sostituire la fase di configurazione predefinita e aggiungere passaggi per scaricare i file di CloudWatch configurazione dal bucket di CloudWatch configurazione S3.

Esaminate il documento InstallAndManageCloudWatchDocumentcompletato.yaml aggiornato e confrontatelo con il documento creato da Quick Setup. Il documento creato dal Quick Setup potrebbe essere diverso, quindi assicurati di aver apportato le modifiche necessarie. Modifica il documento esistente per includere i passaggi e le modifiche necessari.

## Usa CloudFormation al posto di Quick Setup

Invece di utilizzare Quick Setup, è possibile utilizzare CloudFormation per configurare Systems Manager. Questo approccio consente di personalizzare la configurazione di Systems Manager in base ai requisiti specifici. Questo approccio evita inoltre gli aggiornamenti manuali alle risorse Systems Manager configurate create da Quick Setup per supportare CloudWatch configurazioni personalizzate.

La funzionalità Quick Setup utilizza CloudFormation e crea anche un set di CloudFormation stack per distribuire e configurare le risorse di Systems Manager in base alle scelte dell'utente. Prima di poter utilizzare i set di CloudFormation stack, è necessario creare i ruoli IAM utilizzati da CloudFormation StackSets per supportare le distribuzioni su più account o regioni. Quick Setup crea i ruoli necessari per supportare implementazioni multiregionali o multi-account. CloudFormation StackSets È necessario completare i prerequisiti per CloudFormation StackSets configurare e distribuire le risorse di Systems Manager in più regioni o più account da un unico account e regione. Per ulteriori informazioni su questo argomento, vedere Prerequisiti per le operazioni di stack set nella documentazione. CloudFormation

Consulta il CloudFormation modello AWS- QuickSetup - SSMHost Mgmt.yaml per una configurazione rapida personalizzata.

È necessario esaminare le risorse e le funzionalità del CloudFormation modello e apportare modifiche in base alle proprie esigenze. È necessario controllare la versione del CloudFormation modello utilizzato e testare in modo incrementale le modifiche per confermare il risultato richiesto. Inoltre,

è necessario eseguire revisioni della sicurezza del cloud per determinare se sono necessari aggiustamenti delle politiche in base ai requisiti dell'organizzazione.

È necessario distribuire lo CloudFormation stack in un unico account di test e in un'unica regione ed eseguire tutti i casi di test necessari per personalizzare e confermare il risultato desiderato. È quindi possibile estendere la distribuzione a più regioni in un unico account e quindi a più account e più aree.

## Configurazione rapida personalizzata in un unico account e regione con uno CloudFormation stack

Se utilizzi solo un account e una sola regione, puoi distribuire l'esempio completo come CloudFormation stack anziché come set di stack. CloudFormation Tuttavia, se possibile, ti consigliamo di utilizzare l'approccio del set di stack multiaccount e multiregione anche se utilizzi solo un account e una regione singoli. L'utilizzo CloudFormation StackSets semplifica l'espansione ad account e regioni aggiuntivi in futuro.

Utilizza i seguenti passaggi per distribuire il CloudFormation modello AWS- QuickSetup - SSMHost Mgmt.yaml come CloudFormation stack in un singolo account e: Regione AWS

1. Scarica il modello e inseriscilo nel tuo sistema di controllo della versione preferito (ad esempio,). GitHub
2. Personalizza i valori CloudFormation dei parametri predefiniti in base ai requisiti della tua organizzazione.
3. Personalizza gli orari delle associazioni di State Manager.
4. Personalizza il documento Systems Manager con l'ID `InstallAndManageCloudWatchDocument` logico. Verifica che i prefissi del bucket S3 siano allineati ai prefissi del bucket S3 contenente la configurazione. CloudWatch
5. Recupera e registra l'Amazon Resource Name (ARN) per il bucket S3 contenente le tue configurazioni. CloudWatch Per ulteriori informazioni su questo argomento, consulta la Gestione delle configurazioni CloudWatch sezione di questa guida. È disponibile un CloudFormation modello cloudwatch-config-s3-bucket.yaml di esempio che include una policy sui bucket per fornire l'accesso in lettura agli account. AWS Organizations
6. Implementa il CloudFormation modello di configurazione rapida personalizzato sullo stesso account del bucket S3:
   - Per il `CloudWatchConfigBucketARN` parametro, inserisci l'ARN del bucket S3.

- Apportate modifiche alle opzioni dei parametri in base alle funzionalità che desiderate abilitare per Systems Manager.

7. Implementa un'istanza EC2 di test con e senza un ruolo IAM per confermare che l'istanza EC2 funzioni con. CloudWatch

- Applica l'associazione `AttachIAMToInstance` State Manager. Si tratta di un runbook di Systems Manager configurato per essere eseguito in base a una pianificazione. Le associazioni di State Manager che utilizzano i runbook non vengono applicate automaticamente alle nuove istanze EC2 e possono essere configurate per l'esecuzione in base a una pianificazione. Per ulteriori informazioni, vedere Esecuzione di automazioni con trigger utilizzando State Manager nella documentazione di Systems Manager.
- Verifica che all'istanza EC2 sia associato il ruolo IAM richiesto.
- Verifica che l'agente Systems Manager funzioni correttamente confermando che l'istanza EC2 è visibile in Systems Manager.
- Verifica che l' CloudWatch agente funzioni correttamente visualizzando CloudWatch i log e le metriche in base alle CloudWatch configurazioni del tuo bucket S3.

## Configurazione rapida personalizzata in più regioni e più account con CloudFormation StackSets

Se utilizzi più account e regioni, puoi distribuire il modello AWS- QuickSetup - SSMHost Mgmt.yaml CloudFormation come set di stack. È necessario completare i prerequisiti prima di utilizzare i set di stack.CloudFormation StackSet I requisiti variano a seconda che si stiano distribuendo set di stack con autorizzazioni autogestite o gestite dal servizio.

Si consiglia di distribuire set di stack con autorizzazioni gestite dai servizi in modo che i nuovi account ricevano automaticamente la configurazione rapida personalizzata. È necessario distribuire un set di stack gestito dai servizi dall'account di gestione o dall'account amministratore delegato. AWS Organizations È necessario distribuire lo stack set da un account centralizzato utilizzato per l'automazione con privilegi di amministratore delegato, anziché dall'account di gestione. AWS Organizations Ti consigliamo inoltre di testare la distribuzione dello stack set scegliendo come destinazione un'unità organizzativa (OU) di test con un numero singolo o limitato di account in una regione.

1. Completa i passaggi da 1 a 5 indicati nella Configurazione rapida personalizzata in un unico account e regione con uno CloudFormation stack sezione di questa guida.
2. Accedi a Console di gestione AWS, apri la CloudFormation console e scegli Crea StackSet:
   - Scegli Template è pronto e carica un file modello. Carica il CloudFormation modello che hai personalizzato in base alle tue esigenze.
   - Specificate i dettagli del set di stack:
     - Immettete il nome di un set di stack, ad esempio. `StackSet-SSM-QuickSetup`
     - Apportate modifiche alle opzioni dei parametri in base alle funzionalità che desiderate abilitare per Systems Manager.
     - Per il `CloudWatchConfigBucketARN` parametro, inserisci l'ARN per il bucket S3 della tua CloudWatch configurazione.
     - Specificate le opzioni del set di stack, scegliete se utilizzare le autorizzazioni gestite dal servizio con o le autorizzazioni gestite automaticamente. AWS Organizations
       - Se scegli le autorizzazioni gestite automaticamente, inserisci i dettagli del ruolo e del ruolo IAM. AWSCloudFormationStackSetAdministrationRoleAWSCloudFormationStackSetExecutionRole Il ruolo di amministratore deve esistere nell'account e il ruolo di esecuzione deve esistere in ogni account di destinazione
   - Per le autorizzazioni gestite dal servizio con AWS Organizations, si consiglia di eseguire prima la distribuzione su un'unità organizzativa di test anziché sull'intera organizzazione.
     - Scegli se abilitare le distribuzioni automatiche. Ti consigliamo di scegliere Abilitato. Per quanto riguarda il comportamento di rimozione degli account, l'impostazione consigliata è Elimina pile.
   - Per le autorizzazioni autogestite, inserisci l' AWS account IDs per gli account che desideri configurare. È necessario ripetere questa procedura per ogni nuovo account se si utilizzano autorizzazioni gestite automaticamente.
   - Inserisci le regioni in cui utilizzerai CloudWatch e Systems Manager.
   - Verifica che l'implementazione sia avvenuta correttamente visualizzando lo stato nella scheda Operations and Stack Instances per lo stack set.
   - Verifica che Systems Manager e CloudWatch Systems Manager funzionino correttamente negli account distribuiti seguendo il passaggio 7 della Configurazione rapida personalizzata in un unico account e regione con uno CloudFormation stack sezione di questa guida.

# Considerazioni sulla configurazione dei server locali

L' CloudWatch agente per server e macchine virtuali locali viene installato e configurato utilizzando un approccio simile a quello per le istanze EC2. Tuttavia, la tabella seguente fornisce considerazioni da valutare durante l'installazione e la configurazione dell' CloudWatch agente sui server locali e. VMs

| | |
|---|---|
| Indirizzare l' CloudWatch agente sulle stesse credenziali temporanee utilizzate per Systems Manager. | Quando configuri Systems Manager in un ambiente ibrido che include server locali, puoi attivare Systems Manager con un ruolo IAM. È necessario utilizzare il ruolo creato per le istanze EC2 che include le `CloudWatchAgentServerPolicy` politiche e. `AmazonSSMManagedInstanceCore`<br><br>Ciò comporta il recupero e la scrittura di credenziali temporanee da parte dell'agente Systems Manager in un file di credenziali locale. È possibile indirizzare la configurazione CloudWatch dell'agente allo stesso file. È possibile utilizzare il processo di Configurazione dei server locali che utilizzano l'agente Systems Manager e l'agente unificato CloudWatch per utilizzare solo credenziali temporanee nel AWS Knowledge Center.<br><br>È inoltre possibile automatizzare questo processo definendo un runbook di Systems Manager Automation e un'associazione State Manager separati e assegnando tag alle istanze locali. Quando si crea un'attivazione di Systems Manager per le istanze locali, è necessario includere un tag che identifichi le istanze come istanze locali. |

| | |
|---|---|
| Prendi in considerazione l'utilizzo di account e regioni con VPN o Access and. Direct Connect AWS PrivateLink | Puoi usare AWS Direct Connect or AWS Virtual Private Network (Site-to-Site VPN) per stabilire connessioni private tra le reti locali e il tuo cloud privato virtuale (VPC). AWS PrivateLinkstabilisce una connessione privata ai CloudWatch registri con un endpoint VPC di interfaccia. Questo approccio è utile in presenza di restrizioni che impediscono l'invio di dati tramite Internet pubblico a un endpoint di servizio pubblico. |
| Tutte le metriche devono essere incluse nel CloudWatch file di configurazione. | Amazon EC2 include parametri standard (ad esempio l'utilizzo della CPU), ma questi parametri devono essere definiti per le istanze locali. Puoi utilizzare un file di configurazione della piattaforma separato per definire questi parametri per i server locali e quindi aggiungere la configurazione alla configurazione dei parametri standard per la piattaforma. CloudWatch |

## Considerazioni per le istanze EC2 temporanee

Le istanze EC2 sono temporanee o temporanee se vengono fornite da Amazon EC2 Auto Scaling, Amazon EMR, Amazon EC2 Spot Instances oppure. AWS Batch Le istanze EC2 temporanee possono generare un numero molto elevato di flussi in un gruppo di log comune senza informazioni aggiuntive sulla loro origine di runtime. CloudWatch

Se utilizzi istanze EC2 temporanee, valuta la possibilità di aggiungere ulteriori informazioni contestuali dinamiche nei nomi dei gruppi di log e dei flussi di log. Ad esempio, puoi includere l'ID della richiesta dell'istanza Spot, il nome del cluster Amazon EMR o il nome del gruppo Auto Scaling. Queste informazioni possono variare a seconda delle istanze EC2 appena lanciate e potrebbe essere necessario recuperarle e configurarle in fase di esecuzione. È possibile farlo scrivendo un file di configurazione CloudWatch dell'agente all'avvio e riavviando l'agente per includere il file di configurazione aggiornato. Ciò consente l'invio di log e metriche per l' CloudWatchutilizzo di informazioni dinamiche di runtime.

È inoltre necessario assicurarsi che le metriche e i log vengano inviati dall' CloudWatch agente prima che le istanze EC2 temporanee vengano terminate. L' CloudWatch agente include un `flush_interval` parametro che può essere configurato per definire l'intervallo di tempo per lo svuotamento dei buffer di log e metrici. È possibile ridurre questo valore in base al carico di lavoro, arrestare l' CloudWatch agente e forzare lo svuotamento dei buffer prima che l'istanza EC2 venga terminata.

### Utilizzo di una soluzione automatizzata per distribuire l'agente CloudWatch

Se utilizzi una soluzione di automazione (ad esempio, Ansible o Chef), puoi sfruttarla per installare e aggiornare automaticamente l'agente. CloudWatch Se si utilizza questo approccio, è necessario valutare le seguenti considerazioni:

- Verifica che l'automazione copra OSs le versioni del sistema operativo supportate. Se lo script di automazione non supporta tutte le versioni dell'organizzazione OSs, è necessario definire soluzioni alternative per quelle non OSs supportate.
- Verifica che la soluzione di automazione controlli regolarmente gli aggiornamenti e gli CloudWatch upgrade degli agenti. La soluzione di automazione deve verificare regolarmente la presenza di aggiornamenti dell' CloudWatch agente oppure disinstallare e reinstallare regolarmente l'agente. È possibile utilizzare una funzionalità di pianificazione o di una soluzione di automazione per controllare e aggiornare regolarmente l'agente.
- Verifica di poter confermare la conformità dell'installazione e della configurazione dell'agente. La soluzione di automazione dovrebbe consentire di determinare quando un sistema non ha l'agente installato o quando l'agente non funziona. È possibile implementare una notifica o un allarme nella soluzione di automazione in modo da tenere traccia delle installazioni e delle configurazioni non riuscite.

## Distribuzione dell' CloudWatch agente durante il provisioning dell'istanza con lo script dei dati utente

Puoi utilizzare questo approccio se non intendi utilizzare Systems Manager e desideri utilizzarlo in modo selettivo CloudWatch per le tue istanze EC2. In genere, questo approccio viene utilizzato una sola volta o quando è richiesta una configurazione specializzata. AWS fornisce collegamenti diretti all' CloudWatch agente che possono essere scaricati negli script di avvio o nei dati utente. I pacchetti di installazione degli agenti possono essere eseguiti silenziosamente senza l'interazione dell'utente, il

che significa che è possibile utilizzarli in distribuzioni automatizzate. Se si utilizza questo approccio, è necessario valutare le seguenti considerazioni:

- Maggiore rischio che gli utenti non installino l'agente o configurino metriche standard. Gli utenti potrebbero effettuare il provisioning delle istanze senza includere i passaggi necessari per installare l' CloudWatch agente. Potrebbero inoltre configurare erroneamente l'agente, con conseguenti incongruenze nella registrazione e nel monitoraggio.
- Gli script di installazione devono essere specifici del sistema operativo e adatti a diverse versioni del sistema operativo. Sono necessari script separati se si intende utilizzare sia Windows che Linux. Lo script Linux dovrebbe inoltre avere fasi di installazione diverse in base alla distribuzione.
- È necessario aggiornare regolarmente l' CloudWatch agente con nuove versioni quando disponibili. Questa operazione può essere automatizzata se si utilizza Systems Manager con State Manager, ma è anche possibile configurare lo script dei dati utente per eseguirlo nuovamente all'avvio dell'istanza. L' CloudWatch agente viene quindi aggiornato e reinstallato a ogni riavvio.
- È necessario automatizzare il recupero e l'applicazione delle configurazioni standard. CloudWatch Questa operazione può essere automatizzata se si utilizza Systems Manager con State Manager, ma è anche possibile configurare uno script di dati utente per recuperare i file di configurazione all'avvio e riavviare l' CloudWatch agente.

## Includendo l' CloudWatch agente nel tuo AMIs

Il vantaggio dell'utilizzo di questo approccio è che non è necessario attendere l'installazione e la configurazione dell' CloudWatch agente e si può iniziare immediatamente a registrare e monitorare. In questo modo è possibile monitorare meglio le fasi di provisioning e avvio delle istanze nel caso in cui le istanze non si avviino. Questo approccio è appropriato anche se non si prevede di utilizzare l'agente Systems Manager. Se si utilizza questo approccio, è necessario valutare le seguenti considerazioni:

- È necessario che esista un processo di aggiornamento perché AMIs potrebbe non includere la versione dell' CloudWatch agente più recente. L' CloudWatch agente installato in un'AMI è aggiornato solo fino all'ultima volta che l'AMI è stata creata. È necessario includere un metodo aggiuntivo per aggiornare l'agente regolarmente e al momento del provisioning dell'istanza EC2. Se si utilizza Systems Manager, è possibile utilizzare la Installazione dell' CloudWatch agente utilizzando Systems Manager Distributor e State Manager soluzione fornita in questa guida a tale scopo. Se non si utilizza Systems Manager, è possibile utilizzare uno script di dati utente per aggiornare l'agente all'avvio e al riavvio dell'istanza.

- Il file di configurazione CloudWatch dell'agente deve essere recuperato all'avvio dell'istanza. Se non si utilizza Systems Manager, è possibile configurare uno script di dati utente per recuperare i file di configurazione all'avvio e quindi riavviare l' CloudWatch agente.
- L' CloudWatch agente deve essere riavviato dopo l'aggiornamento della CloudWatch configurazione.
- AWS le credenziali non devono essere salvate nell'AMI. Assicurati che nessuna AWS credenziale locale sia memorizzata nell'AMI. Se usi Amazon EC2, puoi applicare il ruolo IAM necessario alla tua istanza ed evitare le credenziali locali. Se utilizzi istanze locali, devi automatizzare o aggiornare manualmente le credenziali dell'istanza prima di avviare l'agente. CloudWatch

# Registrazione e monitoraggio su Amazon ECS

Amazon Elastic Container Service (Amazon ECS) offre due tipi di avvio per l'esecuzione di container e che determinano il tipo di infrastruttura che ospita attività e servizi; questi tipi di avvio sono AWS Fargate Amazon EC2. Entrambi i tipi di avvio si integrano CloudWatch , ma le configurazioni e il supporto variano.

Le seguenti sezioni ti aiutano a capire come utilizzare CloudWatch per la registrazione e il monitoraggio su Amazon ECS.

Argomenti



## Configurazione CloudWatch con un tipo di avvio EC2

Con un tipo di lancio EC2, esegui il provisioning di un cluster Amazon ECS di istanze EC2 che utilizzano l' CloudWatchagente per la registrazione e il monitoraggio. Un'AMI ottimizzata per Amazon ECS viene preinstallata con l'agente container Amazon ECS e fornisce CloudWatch parametri per il cluster Amazon ECS.

Questi parametri predefiniti sono inclusi nel costo di Amazon ECS, ma la configurazione predefinita per Amazon ECS non monitora i file di log o parametri aggiuntivi (ad esempio, spazio libero su disco). Puoi utilizzare il Console di gestione AWS per effettuare il provisioning di un cluster Amazon ECS con il tipo di avvio EC2, in modo da creare uno CloudFormation stack che distribuisce un Amazon EC2 Auto Scaling gruppo con una configurazione di avvio. Tuttavia, questo approccio significa che non è possibile scegliere un'AMI personalizzata o personalizzare la configurazione di avvio con impostazioni diverse o script di avvio aggiuntivi.

Per monitorare log e parametri aggiuntivi, devi installare l' CloudWatch agente sulle tue istanze di container Amazon ECS. Puoi utilizzare l'approccio di installazione per le istanze EC2 descritto nella sezione di questa guida. Installazione dell' CloudWatch agente utilizzando Systems Manager Distributor e State Manager Tuttavia, l'AMI Amazon ECS non include l'agente Systems Manager

richiesto. È necessario utilizzare una configurazione di avvio personalizzata con uno script di dati utente che installi l'agente Systems Manager quando si crea il cluster Amazon ECS. Ciò consente alle istanze del contenitore di registrarsi con Systems Manager e applicare le associazioni di State Manager per installare, configurare e aggiornare l' CloudWatch agente. Quando State Manager esegue e aggiorna la configurazione CloudWatch dell'agente, applica anche la configurazione standardizzata a livello di sistema per Amazon CloudWatch EC2. Puoi anche archiviare CloudWatch configurazioni standardizzate per Amazon ECS nel bucket S3 per la tua CloudWatch configurazione e applicarle automaticamente con State Manager.

È necessario assicurarsi che il ruolo o il profilo dell'istanza IAM applicato alle istanze di container Amazon ECS includa i requisiti `CloudWatchAgentServerPolicy` e `AmazonSSMManagedInstanceCore` le policy. Puoi utilizzare il modello ecs_cluster_with_cloudwatch_linux.yaml per effettuare il provisioning di cluster Amazon CloudFormation ECS basati su Linux. Questo modello crea un cluster Amazon ECS con una configurazione di avvio personalizzata che installa Systems Manager e distribuisce una CloudWatch configurazione personalizzata per monitorare i file di registro specifici di Amazon ECS.

È necessario acquisire i seguenti log per le istanze di container Amazon ECS, oltre ai log delle istanze EC2 standard:

- Output di avvio dell'agente Amazon ECS — `/var/log/ecs/ecs-init.log`
- Output dell'agente Amazon ECS: `/var/log/ecs/ecs-agent.log`
- Registro delle richieste del provider di credenziali IAM: `/var/log/ecs/audit.log`

Per ulteriori informazioni sul livello di output, sulla formattazione e sulle opzioni di configurazione aggiuntive, consulta le posizioni dei file di log di Amazon ECS nella documentazione di Amazon ECS.

> **Important**
>
> L'installazione o la configurazione dell'agente non è richiesta per il tipo di avvio Fargate perché non si eseguono o gestiscono istanze di container EC2.

Le istanze di container Amazon ECS devono utilizzare l'agente contenitore AMIs e ottimizzato per Amazon ECS più recente. AWS archivia i parametri pubblici di Systems Manager Parameter Store con informazioni AMI ottimizzate per Amazon ECS, incluso l'ID AMI. Puoi recuperare l'AMI ottimizzata più recente da Parameter Store utilizzando il formato dei parametri Parameter Store per Amazon

ECS ottimizzato. AMIs Puoi fare riferimento al parametro pubblico Parameter Store che fa riferimento all'AMI più recente o a una versione AMI specifica nei tuoi CloudFormation modelli.

AWS fornisce gli stessi parametri Parameter Store in ogni regione supportata. Ciò significa che i CloudFormation modelli che fanno riferimento a questi parametri possono essere riutilizzati tra regioni e account senza che l'AMI venga aggiornato. Puoi controllare la distribuzione di una nuova AMI Amazon ECS nella tua organizzazione facendo riferimento AMIs a una versione specifica, che ti aiuta a prevenire l'uso di una nuova AMI ottimizzata per Amazon ECS fino a quando non la testerai.

# Registri dei container Amazon ECS per i tipi di lancio EC2 e Fargate

Amazon ECS utilizza una definizione di attività per distribuire e gestire contenitori come attività e servizi. Configura i contenitori che desideri avviare nel tuo cluster Amazon ECS all'interno di una definizione di attività. La registrazione è configurata con un driver di registro a livello di contenitore. Diverse opzioni di driver di registro forniscono ai contenitori diversi sistemi di registrazione (ad esempio,`awslogs`,`fluentd`,,`gelf`,`json-file`, `journald` `logentries` `splunksyslog`, o`awsfirelens`) a seconda che si utilizzi il tipo di avvio EC2 o Fargate. Il tipo di avvio Fargate fornisce un sottoinsieme delle seguenti opzioni del driver di registro:`awslogs`,, `splunk` e. `awsfirelens` AWS fornisce il driver di `awslogs` registro per acquisire e trasmettere l'output del contenitore a CloudWatch Logs. Le impostazioni del driver di registro consentono di personalizzare il gruppo di log, la regione e il prefisso del flusso di log insieme a molte altre opzioni.

La denominazione predefinita per i gruppi di log e l'opzione utilizzata dall'opzione Configurazione automatica dei CloudWatch registri su è. Console di gestione AWS `/ecs/<task_name>` Il nome del flusso di log utilizzato da Amazon ECS ha il `<awslogs-stream-prefix>/<container_name>/<task_id>` formato. Ti consigliamo di utilizzare un nome di gruppo che raggruppi i log in base ai requisiti dell'organizzazione. Nella tabella seguente, gli `image_name` e `image_tag` sono inclusi nel nome del flusso di log.

| | |
|---|---|
| Nome del gruppo di log | `/<Business unit>/<Project or application name>/<Environment>/<Cluster name>/<Task name>` |
| Prefisso del nome del flusso di registro | `/<image_name>/<image_tag>` |

Queste informazioni sono disponibili anche nella definizione dell'attività. Tuttavia, le attività vengono aggiornate regolarmente con nuove revisioni, il che significa che la definizione dell'attività potrebbe aver utilizzato un `image_name` e `image_tag` diverso da quelli attualmente utilizzati dalla definizione dell'attività. Per ulteriori informazioni e suggerimenti di denominazione, consulta la Pianificazione dell' CloudWatch implementazione sezione di questa guida.

Se si utilizza un CI/CD) pipeline or automated process, you can create a new task definition revision for your application with each new Docker image build. For example, you can include the Docker image name, image tag, GitHub revision, or other important information in your task definition revision and logging configuration as a part of your CI/CD processo di integrazione e distribuzione continua ().

# Utilizzo del routing di log personalizzato con FireLens per Amazon ECS

FireLens per Amazon ECS ti aiuta a indirizzare i log verso Fluentd o Fluent Bit in modo da poter inviare direttamente i log dei container ai AWS servizi e alle destinazioni AWS Partner Network (APN), oltre a supportare la spedizione dei log a Logs. CloudWatch

AWS fornisce un'immagine Docker per Fluent Bit con plugin preinstallati per Amazon Kinesis Data Streams, Amazon Data Firehose e Logs. CloudWatch Puoi utilizzare il driver di registro anziché il driver di FireLens registro per una maggiore personalizzazione e `awslogs` controllo dei log inviati a Logs. CloudWatch

Ad esempio, è possibile utilizzare il driver di FireLens registro per controllare l'output in formato di registro. Ciò significa che i CloudWatch log di un contenitore Amazon ECS vengono formattati automaticamente come oggetti JSON e includono proprietà in formato JSON per,,, e. `ecs_cluster` `ecs_task_arn` `ecs_task_definition` `container_id` `container_name` `ec2_instance_id` L'host fluente viene esposto al contenitore tramite le variabili di ambiente e quando si specifica il `FLUENT_HOST` driver. `FLUENT_PORT` `awsfirelens` Ciò significa che puoi accedere direttamente al log router dal tuo codice utilizzando le librerie Fluent Logger. Ad esempio, l'applicazione potrebbe includere la `fluent-logger-python` libreria per accedere a Fluent Bit utilizzando i valori disponibili nelle variabili di ambiente.

Se scegli di utilizzarlo FireLens per Amazon ECS, puoi configurare le stesse impostazioni del driver di `awslogs` registro e utilizzare anche altre impostazioni. Ad esempio, puoi utilizzare la definizione di task ecs-task-nginx-firelenseAmazon ECS .json che avvia un server NGINX configurato per l'uso per la registrazione. FireLens CloudWatch Lancia anche un contenitore FireLens Fluent Bit come sidecar per la registrazione.

# Metriche per Amazon ECS

Amazon ECS fornisce CloudWatch metriche standard (ad esempio, utilizzo della CPU e della memoria) per i tipi di lancio di EC2 e Fargate a livello di cluster e di servizio con l'agente container Amazon ECS. Puoi anche acquisire metriche per i tuoi servizi, attività e contenitori utilizzando CloudWatch Container Insights o acquisire parametri personalizzati dei contenitori utilizzando il formato metrico incorporato.

Container Insights è una CloudWatch funzionalità che fornisce metriche come l'utilizzo della CPU, l'utilizzo della memoria, il traffico di rete e lo storage a livello di cluster, istanza di contenitore, servizio e attività. Container Insights crea anche dashboard automatici che consentono di analizzare servizi e attività e visualizzare l'utilizzo medio della memoria o della CPU a livello di contenitore. Container Insights pubblica metriche personalizzate nello spazio dei nomi `ECS/ContainerInsights` personalizzato che puoi utilizzare per la creazione di grafici, allarmi e dashboard.

Puoi attivare i parametri di Container Insight abilitando Container Insights per ogni singolo cluster Amazon ECS. Se desideri visualizzare anche i parametri a livello di istanza del contenitore, puoi avviare l' CloudWatch agente come contenitore daemon sul tuo cluster Amazon ECS. Puoi utilizzare il CloudFormation modello cwagent-ecs-instance-metric-cfn.yaml per distribuire l'agente CloudWatch come servizio Amazon ECS. È importante sottolineare che questo esempio presuppone che tu abbia creato una configurazione dell' CloudWatchagente personalizzata appropriata e l'abbia archiviata in Parameter Store con la chiave. `ecs-cwagent-daemon-service`

L'CloudWatchagente distribuito come contenitore daemon per CloudWatch Container Insights include parametri aggiuntivi su disco, memoria e CPU come `instance_cpu_reserved_capacity` e `instance_memory_reserved_capacity` con le dimensioni,. `ClusterName` `ContainerInstanceId` `InstanceId` Le metriche a livello di istanza del contenitore vengono implementate da Container Insights utilizzando il formato metrico incorporato. CloudWatch Puoi configurare parametri aggiuntivi a livello di sistema per le tue istanze di container Amazon ECS utilizzando l'approccio descritto nella sezione di questa guida. Configura State Manager and Distributor per CloudWatch la distribuzione e la configurazione degli agenti

## Creazione di parametri applicativi personalizzati in Amazon ECS

Puoi creare parametri personalizzati per le tue applicazioni utilizzando il formato metrico CloudWatchincorporato. Il driver di `awslogs` registro può interpretare le istruzioni in formato metrico CloudWatch incorporato.

La variabile di `CW_CONFIG_CONTENT` ambiente nell'esempio seguente è impostata sul contenuto del parametro `cwagentconfig` Systems Manager Parameter Store. È possibile eseguire l'agente con questa configurazione di base per configurarlo come endpoint in formato metrico incorporato. Tuttavia, non è più necessario.

```
  {
  "logs": {
    "metrics_collected": {
      "emf": { }
    }
  }
}
```

Se disponi di distribuzioni Amazon ECS su più account e regioni, puoi utilizzare un Gestione dei segreti AWS segreto per archiviare la CloudWatch configurazione e configurare la policy segreta per condividerla con la tua organizzazione. Puoi utilizzare l'opzione secrets nella definizione dell'attività per impostare la variabile. `CW_CONFIG_CONTENT`

Puoi utilizzare le librerie di formati metrici incorporati open source AWS fornite nell'applicazione e specificare la variabile di `AWS_EMF_AGENT_ENDPOINT` ambiente da connettere al contenitore laterale dell' CloudWatch agente che funge da endpoint in formato metrico incorporato. Ad esempio, puoi utilizzare l'applicazione Python di esempio ecs_cw_emf_example per inviare metriche in formato metrico incorporato a un contenitore sidecar dell'agente configurato come endpoint in formato metrico incorporato. CloudWatch

Il plug-in Fluent Bit per può essere utilizzato anche per inviare messaggi in formato metrico incorporato. CloudWatch Puoi anche utilizzare l'applicazione Python di esempio ecs_firelense_emf_example per inviare metriche in formato metrico incorporato a un contenitore sidecar Firelens for Amazon ECS.

Se non desideri utilizzare il formato metrico incorporato, puoi creare e aggiornare i parametri tramite l'API o l'SDK. CloudWatch AWSAWS Non consigliamo questo approccio a meno che tu non abbia un caso d'uso specifico, perché aggiunge un sovraccarico di manutenzione e gestione al codice.

# Registrazione e monitoraggio su Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) si CloudWatch integra con Logs per il piano di controllo Kubernetes. Il piano di controllo viene fornito come servizio gestito da Amazon EKS e puoi attivare la registrazione senza installare un CloudWatch agente. L' CloudWatch agente può anche essere distribuito per acquisire i log dei nodi e dei container di Amazon EKS. Fluent Bit e Fluentd sono supportati anche per l'invio dei log dei container a Logs. CloudWatch

CloudWatch Container Insights fornisce una soluzione completa di monitoraggio delle metriche per Amazon EKS a livello di cluster, nodo, pod, task e servizio. Amazon EKS supporta anche diverse opzioni per l'acquisizione di metriche con Prometheus. Il piano di controllo di Amazon EKS fornisce un endpoint di metriche che espone le metriche in un formato Prometheus. Puoi implementare Prometheus nel tuo cluster Amazon EKS per utilizzare questi parametri.

Puoi anche configurare l' CloudWatch agente per acquisire le metriche di Prometheus e CloudWatch creare metriche, oltre a utilizzare altri endpoint Prometheus. Il monitoraggio di Container Insights per Prometheus può anche rilevare e acquisire automaticamente le metriche di Prometheus da carichi di lavoro e sistemi containerizzati supportati.

Puoi installare e configurare l' CloudWatch agente sui tuoi nodi Amazon EKS, in modo simile all'approccio utilizzato per Amazon EC2 con Distributor e State Manager, per allineare i nodi Amazon EKS alle configurazioni standard di registrazione e monitoraggio del sistema.

## Registrazione per Amazon EKS

La registrazione di Kubernetes può essere suddivisa in registrazione del piano di controllo, registrazione dei nodi e registrazione delle applicazioni. Il piano di controllo Kubernetes è un insieme di componenti che gestiscono i cluster Kubernetes e producono log utilizzati per scopi di controllo e diagnostica. Con Amazon EKS, puoi attivare i log per diversi componenti del piano di controllo e inviarli a CloudWatch.

Kubernetes esegue anche componenti di sistema come `kubelet` e `kube-proxy` su ogni nodo Kubernetes che esegue i tuoi pod. Questi componenti scrivono i log all'interno di ogni nodo e puoi configurare CloudWatch Container Insights per acquisire questi log per ogni nodo Amazon EKS.

I container sono raggruppati come pod all'interno di un cluster Kubernetes e sono programmati per essere eseguiti sui tuoi nodi Kubernetes. La maggior parte delle applicazioni containerizzate scrive su standard output e standard error e il motore del contenitore reindirizza l'output a un driver di

registrazione. In Kubernetes, i log del contenitore si trovano nella directory di un nodo. `/var/log/pods` Puoi configurare CloudWatch Container Insights per acquisire questi log per ciascuno dei tuoi pod Amazon EKS.

## Logging del piano di controllo di Amazon EKS

Un cluster Amazon EKS è costituito da un piano di controllo single-tenant ad alta disponibilità per il cluster Kubernetes e i nodi Amazon EKS che eseguono i container. I nodi del piano di controllo vengono eseguiti in un account gestito da. AWS I nodi del piano di controllo del cluster Amazon EKS sono integrati con CloudWatch e puoi attivare la registrazione per componenti specifici del piano di controllo.

I log vengono forniti per ogni istanza del componente del piano di controllo Kubernetes. AWS gestisce lo stato dei nodi del piano di controllo e fornisce un accordo sul livello di servizio (SLA) per l'endpoint Kubernetes.

## Registrazione di nodi e applicazioni Amazon EKS

Ti consigliamo di utilizzare CloudWatchContainer Insights per acquisire log e metriche per Amazon EKS. Container Insights implementa metriche a livello di cluster, nodo e pod con l' CloudWatch agente e Fluent Bit o Fluentd per l'acquisizione dei log. CloudWatch Container Insights fornisce anche dashboard automatici con viste a più livelli delle metriche acquisite. CloudWatch Container Insights viene distribuito come CloudWatch DaemonSet Fluent Bit DaemonSet che viene eseguito su ogni nodo Amazon EKS. I nodi Fargate non sono supportati da Container Insights perché i nodi sono gestiti AWS e non supportano. DaemonSets La registrazione di Fargate per Amazon EKS è trattata separatamente in questa guida.

La tabella seguente mostra i gruppi di CloudWatch log e i log acquisiti dalla configurazione di acquisizione dei log predefinita di Fluentd o Fluent Bit per Amazon EKS.

| | |
|---|---|
| `/aws/containerinsights/Cluster_Name/application` | Tutti i file di log inseriti. `/var/log/containers` Questa directory fornisce collegamenti simbolici a tutti i log dei contenitori Kubernetes nella struttura delle cartelle. `/var/log/pods` Questo cattura i log del contenitore dell'applicazione che scrivono su o. |

| | |
|---|---|
| | `stdout` `stderr` Include anche i log per i contenitori del sistema Kubernetes come, e. `aws-vpc-cni-init` `kube-proxy` `coreDNS` |
| `/aws/containerinsights/Cluster_Name/host` | Registri da, e. `/var/log/dmesg` `/var/log/secure` `/var/log/messages` |
| `/aws/containerinsights/Cluster_Name/dataplane` | I log in `/var/log/journal` per `kubelet.service` `kubeproxy.service` e `docker.service` . |

Se non desideri utilizzare Container Insights con Fluent Bit o Fluentd per la registrazione, puoi acquisire i log dei nodi e dei container con l'agente CloudWatch installato sui nodi Amazon EKS. I nodi Amazon EKS sono istanze EC2, il che significa che dovresti includerli nel tuo approccio di registrazione standard a livello di sistema per Amazon EC2. Se installi l' CloudWatch agente utilizzando Distributor e State Manager, i nodi Amazon EKS vengono inclusi anche nell'installazione, nella configurazione e nell'aggiornamento dell' CloudWatch agente.

La tabella seguente mostra i log specifici di Kubernetes e che devi acquisire se non utilizzi Container Insights con Fluent Bit o Fluentd per la registrazione.

| | |
|---|---|
| `/var/log/containers` | Questa directory fornisce collegamenti simbolici a tutti i log dei contenitori Kubernetes all'interno della struttura di directory. `/var/log/pods` Questo cattura efficacemente i log del contenitore dell'applicazione che scrivono su o. `stdout` `stderr` Ciò include i log per i contenitori del sistema Kubernetes come, e. `aws-vpc-cni-init` `kube-proxy` `coreDNS` Importante: questo non è necessario se si utilizza Container Insights. |
| `var/log/aws-routed-eni/ipamd.log` | I log del demone L-IPAM sono disponibili qui |

| | |
|---|---|
| `/var/log/aws-routed-eni/plugin.log` | |

Devi assicurarti che i nodi Amazon EKS installino e configurino l' CloudWatch agente per inviare log e parametri appropriati a livello di sistema. Tuttavia, l'AMI ottimizzata per Amazon EKS non include l'agente Systems Manager. Utilizzando i modelli di avvio, puoi automatizzare l'installazione dell'agente Systems Manager e una CloudWatch configurazione predefinita che acquisisce importanti log specifici di Amazon EKS con uno script di avvio implementato tramite la sezione dati utente. I nodi Amazon EKS vengono distribuiti utilizzando un gruppo Auto Scaling come gruppo di nodi gestiti o come nodi autogestiti.

Con i gruppi di nodi gestiti, si fornisce un modello di avvio che include la sezione dei dati utente per automatizzare l'installazione e la CloudWatch configurazione dell'agente Systems Manager. Puoi personalizzare e utilizzare il modello amazon_eks_managed_node_group_launch_config.yaml per creare un CloudFormation modello di avvio che installa l'agente e l'agente di Systems Manager e aggiunge anche una configurazione di registrazione specifica di Amazon EKS alla directory di configurazione. CloudWatch CloudWatch Questo modello può essere utilizzato per aggiornare il modello di lancio dei gruppi di nodi gestiti Amazon EKS con un approccio infrastructure-as-code (IaC). Ogni aggiornamento del CloudFormation modello fornisce una nuova versione del modello di lancio. È quindi possibile aggiornare il gruppo di nodi per utilizzare la nuova versione del modello e fare in modo che il processo del ciclo di vita gestito aggiorni i nodi senza tempi di inattività. Assicurati che il ruolo e il profilo di istanza IAM applicati al tuo gruppo di nodi gestiti includano le policy `CloudWatchAgentServerPolicy` gestite `AmazonSSMManagedInstanceCore` AWS .

Con i nodi autogestiti, esegui il provisioning e gestisci direttamente il ciclo di vita e la strategia di aggiornamento per i tuoi nodi Amazon EKS. I nodi autogestiti consentono di eseguire nodi Windows sul cluster Amazon EKS e su Bottlerocket, insieme ad altre opzioni. Puoi utilizzarli CloudFormation per distribuire nodi autogestiti nei tuoi cluster Amazon EKS, il che significa che puoi utilizzare un approccio IaC e di modifica gestita per i tuoi cluster Amazon EKS. AWS fornisce il amazon-eks-nodegroup CloudFormation modello.yaml che puoi usare così com'è o personalizzare. Il modello fornisce tutte le risorse necessarie per i nodi Amazon EKS in un cluster (ad esempio, un ruolo IAM separato, un gruppo di sicurezza, un gruppo Amazon EC2 Auto Scaling e un modello di lancio). Il amazon-eks-nodegroupmodello.yaml è CloudFormation una versione aggiornata che installa l'agente e l'agente Systems Manager richiesti e aggiunge anche una configurazione di registrazione specifica di Amazon EKS alla directory di configurazione. CloudWatch CloudWatch

### Registrazione per Amazon EKS su Fargate

Con Amazon EKS su Fargate, puoi distribuire i pod senza allocare o gestire i nodi Kubernetes. Ciò elimina la necessità di acquisire log a livello di sistema per i nodi Kubernetes. Per acquisire i log dai tuoi pod Fargate, puoi utilizzare Fluent Bit per inoltrare i log direttamente a. CloudWatch Ciò consente di indirizzare automaticamente i log verso Fargate CloudWatch senza ulteriori configurazioni o un contenitore laterale per i pod Amazon EKS. Per ulteriori informazioni su questo argomento, consulta la registrazione di Fargate nella documentazione di Amazon EKS e Fluent Bit per Amazon EKS nel blog. AWS Questa soluzione acquisisce i flussi `STDOUT` and `STDERR` input/output (I/O) dal contenitore e li invia CloudWatch tramite Fluent Bit, in base alla configurazione Fluent Bit stabilita per il cluster Amazon EKS su Fargate.

## Metriche per Amazon EKS e Kubernetes

Kubernetes fornisce un'API di metrica che consente di accedere ai parametri di utilizzo delle risorse (ad esempio, utilizzo della CPU e della memoria per nodi e pod), ma l'API fornisce solo informazioni e non metriche storiche. point-in-time Il server dei parametri Kubernetes viene in genere utilizzato per le implementazioni di Amazon EKS e Kubernetes per aggregare metriche, fornire informazioni storiche a breve termine sulle metriche e supportare funzionalità come Horizontal Pod Autoscaler.

Amazon EKS espone i parametri del piano di controllo tramite il server API Kubernetes in un formato Prometheus e può acquisire e assimilare questi parametri. CloudWatch CloudWatch e Container Insights possono anche essere configurati per fornire metriche complete di acquisizione, analisi e allarmi per i nodi e i pod Amazon EKS.

### Metriche del piano di controllo Kubernetes

Kubernetes espone le metriche del piano di controllo in un formato Prometheus utilizzando l'endpoint dell'API HTTP. `/metrics` È necessario installare Prometheus nel cluster Kubernetes per rappresentare graficamente e visualizzare queste metriche con un browser Web. Puoi anche importare le metriche esposte dal server dell'API Kubernetes in. CloudWatch

### Metriche di nodi e sistemi per Kubernetes

Kubernetes fornisce il pod Prometheus metrics-server che puoi distribuire ed eseguire sui tuoi cluster Kubernetes per statistiche di CPU e memoria a livello di cluster, nodo e pod. Queste metriche vengono utilizzate con Horizontal Pod Autoscaler e Vertical Pod Autoscaler. CloudWatch può anche fornire queste metriche.

È necessario installare Kubernetes Metrics Server se si utilizza la dashboard di Kubernetes o le scaler automatiche a pod orizzontali e verticali. La dashboard Kubernetes ti aiuta a sfogliare e configurare il cluster Kubernetes, i nodi, i pod e la relativa configurazione e a visualizzare le metriche di CPU e memoria dal Kubernetes Metrics Server.

Le metriche fornite dal Kubernetes Metrics Server non possono essere utilizzate per scopi non di scalabilità automatica (ad esempio, il monitoraggio). Le metriche sono destinate all'analisi e non all'analisi storica. point-in-time La dashboard di Kubernetes implementa le metriche `dashboard-metrics-scraper` per archiviare le metriche dal Kubernetes Metrics Server per un breve periodo di tempo.

Container Insights utilizza una versione containerizzata dell' CloudWatch agente che viene eseguita in un DaemonSet Kubernetes per scoprire tutti i container in esecuzione in un cluster e fornire metriche a livello di nodo. Raccoglie dati sulle prestazioni a ogni livello dello stack di prestazioni. Puoi utilizzare il Quick Start di Quick Starts o configurare Container Insights separatamente. AWS Quick Start imposta il monitoraggio delle metriche con l' CloudWatch agente e la registrazione con Fluent Bit, quindi è necessario implementarlo una sola volta per la registrazione e il monitoraggio.

Poiché i nodi Amazon EKS sono istanze EC2, è necessario acquisire parametri a livello di sistema, oltre ai parametri acquisiti da Container Insights, utilizzando gli standard definiti per Amazon EC2. Puoi utilizzare lo stesso approccio descritto nella Configura State Manager and Distributor per CloudWatch la distribuzione e la configurazione degli agenti sezione di questa guida per installare e configurare l' CloudWatch agente per i tuoi cluster Amazon EKS. Puoi aggiornare il tuo file di CloudWatch configurazione specifico di Amazon EKS per includere i parametri e la configurazione di log specifica di Amazon EKS.

L' CloudWatch agente con supporto Prometheus può rilevare ed estrarre automaticamente le metriche di Prometheus dai carichi di lavoro e dai sistemi containerizzati supportati. Li inserisce come CloudWatch log in formato metrico incorporato per l'analisi con Logs Insights e crea automaticamente le metriche. CloudWatch CloudWatch

> **Important**
>
> È necessario implementare una versione specializzata dell' CloudWatch agente per raccogliere le metriche di Prometheus. Si tratta di un agente separato dall'agente distribuito per Container Insights CloudWatch . Puoi utilizzare l'applicazione Java di esempio prometheus_jmx, che include i file di distribuzione e configurazione per l'agente CloudWatch e la distribuzione del pod Amazon EKS, per dimostrare la scoperta delle metriche di

Prometheus. Per ulteriori informazioni, consulta Configurare un carico di lavoro di Java/JMX esempio su Amazon EKS e Kubernetes nella documentazione. CloudWatch Puoi anche configurare l' CloudWatch agente per acquisire metriche da altri target Prometheus in esecuzione nel tuo cluster Amazon EKS.

## Parametri di applicazione

Puoi creare metriche personalizzate con il formato metrico CloudWatchincorporato. Per importare istruzioni in formato metrico incorporato, è necessario inviare voci in formato metrico incorporato a un endpoint in formato metrico incorporato. L' CloudWatch agente può essere configurato come contenitore sidecar nel tuo pod Amazon EKS. La configurazione dell' CloudWatch agente viene archiviata come Kubernetes ConfigMap e letta dal contenitore sidecar CloudWatch dell'agente per avviare l'endpoint in formato metrico incorporato.

Puoi anche configurare la tua applicazione come target Prometheus e configurare l' CloudWatchagente, con il supporto di Prometheus, per scoprire, acquisire e inserire le tue metriche. CloudWatch Ad esempio, è possibile utilizzare l'esportatore JMX open source con le applicazioni Java per esporre JMX Beans per l'utilizzo di Prometheus da parte dell'agente. CloudWatch

Se non desideri utilizzare il formato metrico incorporato, puoi anche creare e aggiornare le metriche utilizzando l'API o l'SDK. CloudWatch AWSAWS Tuttavia, non consigliamo questo approccio perché combina il monitoraggio e la logica dell'applicazione.

## Metriche per Amazon EKS su Fargate

Fargate effettua automaticamente il provisioning dei nodi Amazon EKS per eseguire i pod Kubernetes in modo da non dover monitorare e raccogliere parametri a livello di nodo. Tuttavia, è necessario monitorare i parametri per i pod in esecuzione sui nodi Amazon EKS su Fargate. Container Insights non è attualmente disponibile per Amazon EKS su Fargate perché richiede le seguenti funzionalità che attualmente non sono supportate:

- DaemonSets non sono attualmente supportati. Container Insights viene distribuito eseguendo l' CloudWatch agente come se fosse DaemonSet su ogni nodo del cluster.
- HostPath i volumi persistenti non sono supportati. Il contenitore dell' CloudWatch agente utilizza i volumi persistenti HostPath come prerequisito per la raccolta dei dati metrici del contenitore.
- Fargate impedisce ai container privilegiati e all'accesso alle informazioni dell'host.

È possibile utilizzare il router di registro integrato per Fargate per inviare istruzioni in formato metrico incorporato a. CloudWatch Il log router utilizza Fluent Bit, che dispone di un CloudWatch plug-in che può essere configurato per supportare istruzioni in formato metrico incorporate.

Puoi recuperare e acquisire parametri a livello di pod per i tuoi nodi Fargate implementando il server Prometheus nel tuo cluster Amazon EKS per raccogliere i parametri dai tuoi nodi Fargate. Poiché Prometheus richiede uno storage persistente, puoi distribuire Prometheus su Fargate se utilizzi Amazon Elastic File System (Amazon EFS) per lo storage persistente. Puoi anche distribuire Prometheus su un nodo supportato da Amazon EC2. Per ulteriori informazioni, consulta Monitoring Amazon EKS sull' AWS Fargate uso di Prometheus e Grafana sul blog. AWS

# Monitoraggio di Prometheus su Amazon EKS

Amazon Managed Service for Prometheus fornisce un servizio scalabile, sicuro e gestito per Prometheus open source. AWS È possibile utilizzare il linguaggio di interrogazione Prometheus (PromQL) per monitorare le prestazioni dei carichi di lavoro containerizzati senza gestire l'infrastruttura sottostante per l'acquisizione, l'archiviazione e l'interrogazione delle metriche operative. Puoi raccogliere i parametri di Prometheus da Amazon EKS e Amazon ECS utilizzando i server Distro OpenTelemetry for (ADOT) o AWS Prometheus come agenti di raccolta.

CloudWatch Il monitoraggio di Container Insights per Prometheus ti consente di configurare e utilizzare l' CloudWatch agente per scoprire i parametri di Prometheus dai carichi di lavoro Amazon ECS, Amazon EKS e Kubernetes e inserirli come parametri. CloudWatch CloudWatch Questa soluzione è appropriata se rappresenta la soluzione principale per l'osservabilità e il monitoraggio. Tuttavia, il seguente elenco descrive i casi d'uso in cui Amazon Managed Service for Prometheus offre maggiore flessibilità per l'acquisizione, l'archiviazione e l'interrogazione delle metriche di Prometheus:

- Amazon Managed Service for Prometheus ti consente di utilizzare i server Prometheus esistenti distribuiti in Amazon EKS o Kubernetes autogestiti e di configurarli per scrivere su Amazon Managed Service for Prometheus anziché su un data store configurato localmente. In questo modo si elimina l'onere indifferenziato della gestione di un archivio dati ad alta disponibilità per i server Prometheus e la relativa infrastruttura. Amazon Managed Service for Prometheus è la scelta ideale se disponi di una distribuzione Prometheus matura che desideri sfruttare nel cloud. AWS
- Grafana supporta direttamente Prometheus come fonte di dati per la visualizzazione. Se desideri utilizzare Grafana con Prometheus anziché CloudWatch Dashboards per il monitoraggio dei container, Amazon Managed Service for Prometheus potrebbe soddisfare le tue esigenze. Amazon Managed Service for Prometheus si integra con Amazon Managed Grafana per fornire una soluzione gestita di monitoraggio e visualizzazione open source.
- Prometheus consente di eseguire analisi sulle metriche operative utilizzando le query PromQL. Al contrario, l' CloudWatch agente inserisce le metriche di Prometheus in formato metrico incorporato nei log, che generano metriche. CloudWatch CloudWatch È possibile interrogare i log in formato metrico incorporato utilizzando Logs Insights. CloudWatch
- Se non intendi utilizzarlo CloudWatch per il monitoraggio e l'acquisizione delle metriche, allora dovresti usare Amazon Managed Service for Prometheus con il tuo server Prometheus e una soluzione di visualizzazione come Grafana. È necessario configurare il server Prometheus per acquisire le metriche dai target Prometheus e configurare il server per la scrittura remota nell'area

di lavoro Amazon Managed Service for Prometheus. Se utilizzi Amazon Managed Grafana, puoi integrare direttamente Amazon Managed Grafana con la tua fonte di dati Amazon Managed Service for Prometheus utilizzando il plug-in incluso. Poiché i dati metrici sono archiviati in Amazon Managed Service for Prometheus, non vi è alcuna dipendenza dall'implementazione dell'agente o la necessità di importare i dati. CloudWatch CloudWatch L' CloudWatch agente è necessario per il monitoraggio di Container Insights per Prometheus.

Puoi anche utilizzare ADOT Collector per eseguire lo scraping da un'applicazione basata su Prometheus e inviare i parametri ad Amazon Managed Service for Prometheus. Per ulteriori informazioni su ADOT Collector, consulta la Distro per la documentazione.AWS OpenTelemetry

# Registrazione e metriche per AWS Lambda

Lambda elimina la necessità di gestire e monitorare i server per i carichi di lavoro e funziona automaticamente con CloudWatch Metrics and CloudWatch Logs senza ulteriore configurazione o strumentazione del codice dell'applicazione. Questa sezione ti aiuta a comprendere le caratteristiche prestazionali dei sistemi utilizzati da Lambda e come le tue scelte di configurazione influiscono sulle prestazioni. Inoltre, consente di registrare e monitorare le funzioni Lambda per l'ottimizzazione delle prestazioni e la diagnosi dei problemi a livello di applicazione.

## Registrazione delle funzioni Lambda

Lambda trasmette automaticamente l'output standard e i messaggi di errore standard da una funzione Lambda a CloudWatch Logs, senza richiedere driver di registrazione. Lambda effettua inoltre automaticamente il provisioning dei contenitori che eseguono la funzione Lambda e li configura per generare messaggi di log in flussi di log separati.

Le chiamate successive della funzione Lambda possono riutilizzare lo stesso contenitore e l'output nello stesso flusso di log. Lambda può anche fornire un nuovo contenitore e inviare l'invocazione a un nuovo flusso di log.

Lambda crea automaticamente un gruppo di log quando la funzione Lambda viene richiamata per la prima volta. Le funzioni Lambda possono avere più versioni e puoi scegliere la versione che desideri eseguire. Tutti i log per le chiamate della funzione Lambda sono archiviati nello stesso gruppo di log. Il nome non può essere modificato ed è nel formato. `/aws/lambda/<YourLambdaFunctionName>` Viene creato un flusso di log separato nel gruppo di log per ogni istanza della funzione Lambda. Lambda ha una convenzione di denominazione standard per i flussi di log che utilizza un formato. `YYYY/MM/DD/[<FunctionVersion>]<InstanceId>` `InstanceId`Viene generato da AWS per identificare l'istanza della funzione Lambda.

Ti consigliamo di formattare i messaggi di registro in formato JSON perché puoi interrogarli più facilmente con CloudWatch Logs Insights. Possono anche essere filtrati ed esportati più facilmente. È possibile utilizzare una libreria di registrazione per semplificare questo processo o scrivere funzioni personalizzate per la gestione dei log. Si consiglia di utilizzare una libreria di registrazione per facilitare la formattazione e la classificazione dei messaggi di registro. Ad esempio, se la tua funzione Lambda è scritta in Python, puoi usare il modulo di registrazione Python per registrare i messaggi e controllare il formato di output. Lambda utilizza nativamente la libreria di registrazione Python per le funzioni Lambda scritte in Python e puoi recuperare e personalizzare il logger all'interno della tua

funzione Lambda. AWS Labs ha creato il toolkit per sviluppatori AWS Lambda Powertools for Python per semplificare l'arricchimento dei messaggi di log con dati chiave come gli avvii a freddo. Il toolkit è disponibile per Python, Java, Typescript e.NET.

Un'altra procedura consigliata consiste nell'impostare il livello di output del registro utilizzando una variabile e regolarlo in base all'ambiente e ai requisiti. Il codice della funzione Lambda, oltre alle librerie utilizzate, potrebbe generare una grande quantità di dati di registro a seconda del livello di output del registro. Ciò può influire sui costi di registrazione e sulle prestazioni.

Lambda consente di impostare le variabili di ambiente per l'ambiente di runtime della funzione Lambda senza aggiornare il codice. Ad esempio, puoi creare una variabile di `LAMBDA_LOG_LEVEL` ambiente che definisce il livello di output del log che puoi recuperare dal tuo codice. L'esempio seguente tenta di recuperare una variabile di `LAMBDA_LOG_LEVEL` ambiente e di utilizzare il valore per definire l'output di registrazione. Se la variabile di ambiente non è impostata, il valore predefinito è il livello. `INFO`

```
import logging
from os import getenv

logger = logging.getLogger()
log_level = getenv("LAMBDA_LOG_LEVEL", "INFO")
level = logging.getLevelName(log_level)
logger.setLevel(level)
```

## Invio di log ad altre destinazioni da CloudWatch

Puoi inviare log ad altre destinazioni (ad esempio, Amazon OpenSearch Service o una funzione Lambda) utilizzando i filtri di abbonamento. Se non utilizzi Amazon OpenSearch Service, puoi utilizzare una funzione Lambda per elaborare i log e inviarli a un AWS servizio di tua scelta utilizzando il. AWS SDKs

Puoi anche utilizzarle SDKs per le destinazioni di log al di fuori del AWS Cloud nella tua funzione Lambda per inviare direttamente le istruzioni di registro a una destinazione di tua scelta. Se scegli questa opzione, ti consigliamo di considerare l'impatto della latenza, del tempo di elaborazione aggiuntivo, della gestione degli errori e dei tentativi e dell'accoppiamento della logica operativa alla funzione Lambda.

# Parametri della funzione Lambda

Lambda consente di eseguire il codice senza gestire o scalare i server e questo elimina quasi il peso del controllo e della diagnostica a livello di sistema. Tuttavia, è comunque importante comprendere le metriche delle prestazioni e delle chiamate a livello di sistema per le funzioni Lambda. Ciò consente di ottimizzare la configurazione delle risorse e migliorare le prestazioni del codice. Il monitoraggio e la misurazione efficaci delle prestazioni possono migliorare l'esperienza utente e ridurre i costi dimensionando adeguatamente le funzioni Lambda. In genere, i carichi di lavoro eseguiti come funzioni Lambda hanno anche metriche a livello di applicazione che devono essere acquisite e analizzate. Lambda supporta direttamente il formato metrico incorporato per semplificare l'acquisizione delle metriche a livello di applicazione. CloudWatch

## Metriche a livello di sistema

Lambda si integra automaticamente con CloudWatch Metrics e fornisce un set di metriche standard per le funzioni Lambda. Lambda fornisce anche una dashboard di monitoraggio separata per ogni funzione Lambda con queste metriche. Due metriche importanti da monitorare sono gli errori e gli errori di invocazione. Comprendere le differenze tra gli errori di invocazione e altri tipi di errore aiuta a diagnosticare e supportare le implementazioni Lambda.

Gli errori di chiamata impediscono l'esecuzione della funzione Lambda. Questi errori si verificano prima dell'esecuzione del codice, quindi non è possibile implementare la gestione degli errori all'interno del codice per identificarli. È invece necessario configurare allarmi per le funzioni Lambda che rilevano questi errori e avvisino i proprietari delle operazioni e dei carichi di lavoro. Questi errori sono spesso correlati a un errore di configurazione o di autorizzazione e possono verificarsi a causa di una modifica della configurazione o delle autorizzazioni. Gli errori di invocazione possono avviare un nuovo tentativo, che causa più chiamate della funzione.

Una funzione Lambda richiamata correttamente restituisce una risposta HTTP 200 anche se la funzione genera un'eccezione. Le funzioni Lambda devono implementare la gestione degli errori e generare eccezioni in modo che la `Errors` metrica acquisisca e identifichi le esecuzioni non riuscite della funzione Lambda. È necessario restituire una risposta formattata dalle chiamate alla funzione Lambda che includa informazioni per determinare se l'esecuzione è fallita completamente, parzialmente o ha avuto successo.

CloudWatch fornisce CloudWatch Lambda Insights che puoi abilitare per una singola funzione Lambda. Lambda Insights raccoglie, aggrega e riepiloga le metriche a livello di sistema (ad esempio,

tempo di CPU, memoria, utilizzo del disco e della rete). Lambda Insights raccoglie, aggrega e riepiloga anche le informazioni diagnostiche (ad esempio, partenze a freddo e arresti degli operatori Lambda) per aiutarti a isolare e risolvere rapidamente i problemi.

Lambda Insights utilizza il formato metrico incorporato per inviare automaticamente informazioni sulle prestazioni al gruppo di `/aws/lambda-insights/` log con un prefisso del nome del flusso di log basato sul nome della funzione Lambda. Questi eventi del registro delle prestazioni creano CloudWatch metriche che sono la base per i dashboard automatici. CloudWatch Ti consigliamo di abilitare Lambda Insights per i test delle prestazioni e gli ambienti di produzione. Le metriche aggiuntive create da Lambda Insights `memory_utilization` includono che aiutano a dimensionare correttamente le funzioni Lambda in modo da evitare di pagare per capacità non richiesta.

## Parametri di applicazione

Puoi anche creare e acquisire i parametri delle tue applicazioni CloudWatch utilizzando il formato metrico incorporato. È possibile sfruttare le librerie AWS fornite per il formato metrico incorporato per creare ed emettere istruzioni in formato metrico incorporato. CloudWatch La struttura di CloudWatch registrazione Lambda integrata è configurata per elaborare ed estrarre istruzioni in formato metrico incorporato formattate in modo appropriato.

# Ricerca e analisi dei log in CloudWatch

Dopo aver acquisito i log e le metriche in un formato e in una posizione coerenti, puoi cercarli e analizzarli per migliorare l'efficienza operativa, oltre a identificare e risolvere i problemi. Ti consigliamo di acquisire i log in un formato ben formato (ad esempio, JSON) per semplificare la ricerca e l'analisi dei log. La maggior parte dei carichi di lavoro utilizza una raccolta di AWS risorse come rete, elaborazione, archiviazione e database. Ove possibile, dovresti analizzare collettivamente le metriche e i log di queste risorse e correlarli per monitorare e gestire efficacemente tutti i tuoi carichi di lavoro. AWS

CloudWatch offre diverse funzionalità per aiutare ad analizzare log e metriche, come CloudWatch Application Insights per definire e monitorare collettivamente metriche e log per un'applicazione su diverse AWS risorse, CloudWatch Anomaly Detection per evidenziare le anomalie delle metriche e CloudWatch Log Insights per cercare e analizzare in modo interattivo i dati di log in CloudWatch Logs.

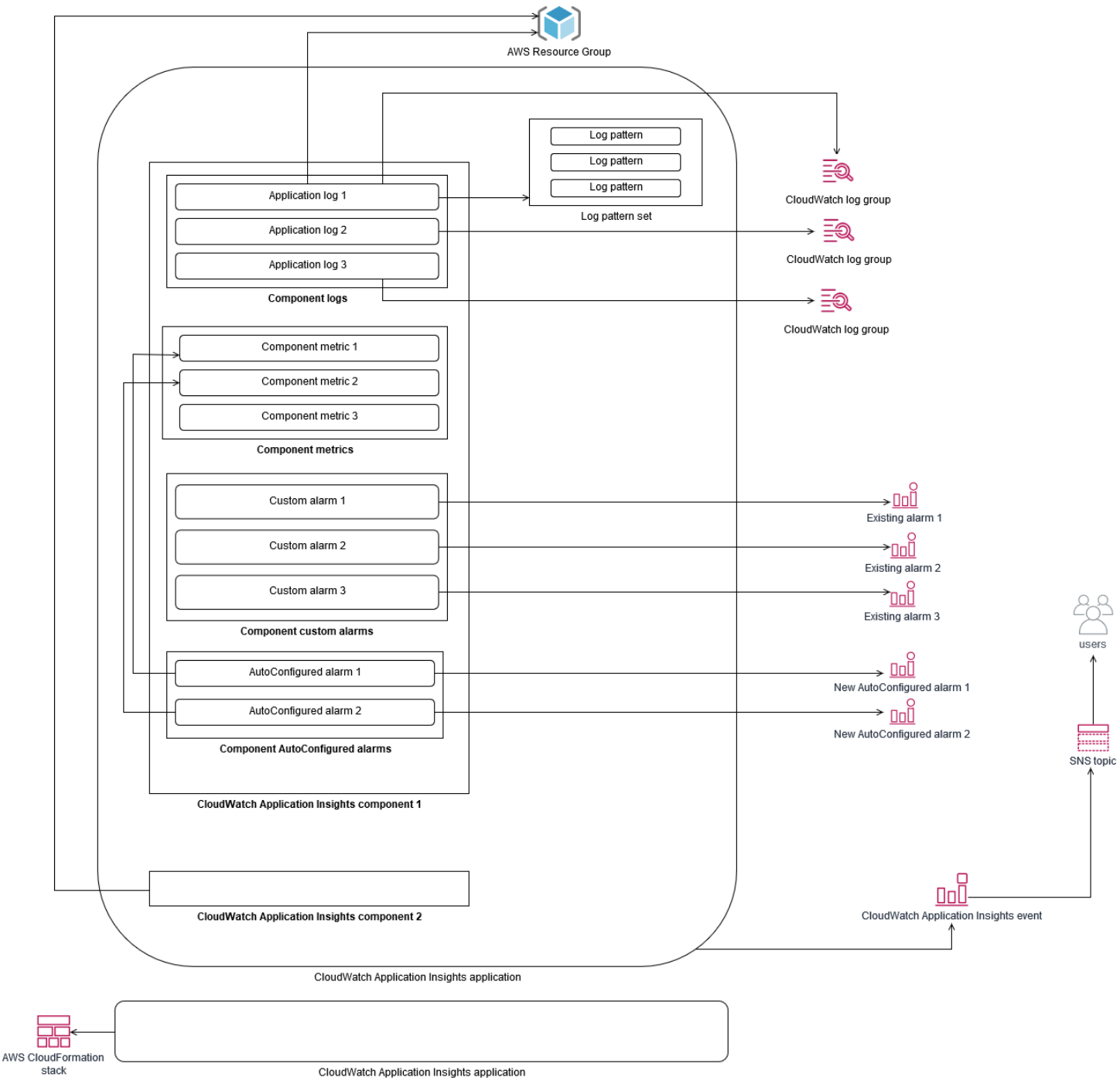
## Monitora e analizza CloudWatch collettivamente le applicazioni con Application Insights

I proprietari delle applicazioni possono utilizzare Amazon CloudWatch Application Insights per configurare il monitoraggio e l'analisi automatici dei carichi di lavoro. Questo può essere configurato in aggiunta al monitoraggio standard a livello di sistema configurato per tutti i carichi di lavoro in un account. L'impostazione del monitoraggio tramite CloudWatch Application Insights può anche aiutare i team applicativi ad allinearsi in modo proattivo alle operazioni e ridurre il tempo medio di ripristino (MTTR). CloudWatch Application Insights può aiutare a ridurre lo sforzo necessario per stabilire la registrazione e il monitoraggio a livello di applicazione. Fornisce inoltre un framework basato su componenti che aiuta i team a dividere le responsabilità di registrazione e monitoraggio.

CloudWatch Application Insights utilizza gruppi di risorse per identificare le risorse che devono essere monitorate collettivamente come applicazione. Le risorse supportate nel gruppo di risorse diventano componenti definiti individualmente dell' CloudWatch applicazione Application Insights. Ogni componente dell' CloudWatch applicazione Application Insights ha i propri registri, metriche e allarmi.

Per i log, si definisce il set di pattern di log da utilizzare per il componente e all'interno dell'applicazione Application Insights. CloudWatch Un set di pattern di log è una raccolta di pattern

di log da cercare in base a espressioni regolari, insieme a una severità bassa, media o alta per il momento in cui viene rilevato il pattern. Per quanto riguarda le metriche, scegli le metriche da monitorare per ogni componente da un elenco di metriche specifiche del servizio e supportate. Per gli allarmi, CloudWatch Application Insights crea e configura automaticamente allarmi standard o di rilevamento delle anomalie per le metriche monitorate. CloudWatch Application Insights dispone di configurazioni automatiche per le metriche e l'acquisizione dei log per le tecnologie descritte nei log e nelle metriche supportate da Application Insights nella documentazione. CloudWatch CloudWatch Il diagramma seguente mostra le relazioni tra i componenti di CloudWatch Application Insights e le relative configurazioni di registrazione e monitoraggio. Ogni componente ha definito i propri log e metriche da monitorare utilizzando log e metriche. CloudWatch




Le istanze EC2 monitorate da CloudWatch Application Insights richiedono Systems Manager, CloudWatch agenti e autorizzazioni. Per ulteriori informazioni a riguardo, consulta Prerequisiti per configurare un' CloudWatch applicazione con Application Insights nella documentazione. CloudWatch CloudWatch Application Insights utilizza Systems Manager per installare e aggiornare l' CloudWatch agente. Le metriche e i log configurati in CloudWatch Application Insights creano un file di configurazione CloudWatch dell'agente archiviato in un parametro Systems Manager con il

`AmazonCloudWatch-ApplicationInsights-SSMParameter` prefisso per ogni componente di CloudWatch Application Insights. Ciò comporta l'aggiunta di un file di configurazione CloudWatch dell'agente separato alla directory di configurazione dell' CloudWatch agente sull'istanza EC2. Viene eseguito un comando Systems Manager per aggiungere questa configurazione alla configurazione attiva sull'istanza EC2. L'utilizzo di CloudWatch Application Insights non influisce sulle impostazioni di configurazione degli CloudWatch agenti esistenti. È possibile utilizzare CloudWatch Application Insights in aggiunta alle configurazioni degli agenti a livello di sistema e di applicazione CloudWatch . Tuttavia, è necessario assicurarsi che le configurazioni non si sovrappongano.

## Esecuzione dell'analisi dei log con CloudWatch Logs Insights

CloudWatch Logs Insights semplifica la ricerca in più gruppi di log utilizzando un semplice linguaggio di interrogazione. Se i log delle applicazioni sono strutturati in formato JSON, CloudWatch Logs Insights rileva automaticamente i campi JSON nei flussi di log in più gruppi di log. È possibile utilizzare CloudWatch Logs Insights per analizzare i log dell'applicazione e del sistema, salvando le query per utilizzi futuri. La sintassi di query per CloudWatch Logs Insights supporta funzioni come l'aggregazione con funzioni, ad esempio sum (), avg (), count (), min () e max (), che possono essere utili per la risoluzione dei problemi delle applicazioni o l'analisi delle prestazioni.

Se utilizzate il formato metrico incorporato per creare CloudWatch metriche, potete interrogare i log in formato metrico incorporato per generare metriche una tantum utilizzando le funzioni di aggregazione supportate. Ciò consente di ridurre i costi di CloudWatch monitoraggio acquisendo i punti dati necessari per generare metriche specifiche in base alle esigenze, anziché acquisirli attivamente come metriche personalizzate. Ciò è particolarmente efficace per le dimensioni con cardinalità elevata che genererebbero un gran numero di metriche. CloudWatch Anche Container Insights adotta questo approccio e acquisisce dati dettagliati sulle prestazioni, ma genera CloudWatch metriche solo per un sottoinsieme di questi dati.

Ad esempio, la seguente voce di metrica incorporata genera solo un set limitato di CloudWatch metriche a partire dai dati metrici acquisiti nell'istruzione Embedded Metric Format:

```
{
 "AutoScalingGroupName": "eks-e0bab7f4-fa6c-64ba-dbd9-094aee6cf9ba",
 "CloudWatchMetrics": [
 {
 "Metrics": [
 {
 "Unit": "Count",
 "Name": "pod_number_of_container_restarts"
```

```
}
],
"Dimensions": [
[
"PodName",
"Namespace",
"ClusterName"
]
],
"Namespace": "ContainerInsights"
}
],
"ClusterName": "eksdemo",
"InstanceId": "i-03b21a16b854aa4ca",
"InstanceType": "t3.medium",
"Namespace": "amazon-cloudwatch",
"NodeName": "ip-172-31-10-211.ec2.internal",
"PodName": "cloudwatch-agent",
"Sources": [
"cadvisor",
"pod",
"calculated"
],
"Timestamp": "1605111338968",
"Type": "Pod",
"Version": "0",
"pod_cpu_limit": 200,
"pod_cpu_request": 200,
"pod_cpu_reserved_capacity": 10,
"pod_cpu_usage_system": 3.268605094109382,
"pod_cpu_usage_total": 8.899539221131045,
"pod_cpu_usage_user": 4.160042847048305,
"pod_cpu_utilization": 0.44497696105655227,
"pod_cpu_utilization_over_pod_limit": 4.4497696105655224,
"pod_memory_cache": 4096,
"pod_memory_failcnt": 0,
"pod_memory_hierarchical_pgfault": 0,
"pod_memory_hierarchical_pgmajfault": 0,
"pod_memory_limit": 209715200,
"pod_memory_mapped_file": 0,
"pod_memory_max_usage": 43024384,
"pod_memory_pgfault": 0,
"pod_memory_pgmajfault": 0,
```

```
 "pod_memory_request": 209715200,
 "pod_memory_reserved_capacity": 5.148439982463127,
 "pod_memory_rss": 38481920,
 "pod_memory_swap": 0,
 "pod_memory_usage": 42803200,
 "pod_memory_utilization": 0.6172094650851303,
 "pod_memory_utilization_over_pod_limit": 11.98828125,
 "pod_memory_working_set": 25141248,
 "pod_network_rx_bytes": 3566.4174629544723,
 "pod_network_rx_dropped": 0,
 "pod_network_rx_errors": 0,
 "pod_network_rx_packets": 3.3495665260575094,
 "pod_network_total_bytes": 4283.442421354973,
 "pod_network_tx_bytes": 717.0249584005006,
 "pod_network_tx_dropped": 0,
 "pod_network_tx_errors": 0,
 "pod_network_tx_packets": 2.6964010534762948,
 "pod_number_of_container_restarts": 0,
 "pod_number_of_containers": 1,
 "pod_number_of_running_containers": 1,
 "pod_status": "Running"
}
```


Tuttavia, puoi interrogare le metriche acquisite per ottenere ulteriori informazioni. Ad esempio, potete eseguire la seguente query per visualizzare gli ultimi 20 pod con errori nelle pagine di memoria:

```
fields @timestamp, @message
| filter (pod_memory_pgfault > 0)
| sort @timestamp desc
| limit 20
```

## Esecuzione dell'analisi dei log con Amazon OpenSearch Service

CloudWatch si integra con Amazon OpenSearch Service consentendoti di trasmettere i dati di log dai gruppi di CloudWatch log a un cluster Amazon OpenSearch Service di tua scelta con un filtro di abbonamento. Puoi utilizzarlo CloudWatch per l'acquisizione e l'analisi di log e metriche principali, quindi aumentarlo con Amazon OpenSearch Service per i seguenti casi d'uso:

- Controllo granulare dell'accesso ai dati: Amazon OpenSearch Service ti consente di limitare l'accesso ai dati fino al livello del campo e aiuta a rendere anonimi i dati nei campi in base alle

autorizzazioni degli utenti. Ciò è utile se desideri supportare la risoluzione dei problemi senza esporre dati sensibili.

- Aggrega e cerca i log su più account, regioni e infrastrutture: puoi trasmettere i log da più account e regioni in un cluster Amazon OpenSearch Service comune. I tuoi team operativi centralizzati possono analizzare tendenze e problemi ed eseguire analisi su più account e regioni. Lo streaming CloudWatch dei log su Amazon OpenSearch Service ti aiuta anche a cercare e analizzare un'applicazione multiregionale in una posizione centrale.
- Spedisci e arricchisci i log direttamente ad Amazon OpenSearch Service utilizzando ElasticSearch agenti: i componenti dello stack applicativo e tecnologico OSs che possono utilizzare non sono supportati dall'agente. CloudWatch Potresti anche voler arricchire e trasformare i dati di log prima che vengano inviati alla tua soluzione di registrazione. Amazon OpenSearch Service supporta client Elasticsearch standard come i data shipper della famiglia Elastic Beats e Logstash che supportano l'arricchimento e la trasformazione dei log prima di inviare i dati di log ad Amazon Service. OpenSearch
- La soluzione di gestione delle operazioni esistente utilizza uno ElasticSearch stack Logstash, Kibana (ELK) per la registrazione e il monitoraggio: potresti già avere un investimento significativo in Amazon OpenSearch Service o Elasticsearch open source con molti carichi di lavoro già configurati. Potresti anche avere dashboard operative create in Kibana che desideri continuare a utilizzare.

Se non prevedi di utilizzare CloudWatch i log, puoi utilizzare agenti, driver di log e librerie supportati da Amazon OpenSearch Service (ad esempio, Fluent Bit, Fluentd, logstash e Open Distro for ElasticSearch API) per inviare i log direttamente ad Amazon Service e bypassarli. OpenSearch CloudWatch Tuttavia, dovresti anche implementare una soluzione per acquisire i log generati dai servizi. AWS CloudWatch Logs è la soluzione di acquisizione dei log principale per molti AWS servizi e più servizi creano automaticamente nuovi gruppi di log. CloudWatch Ad esempio, Lambda crea un nuovo gruppo di log per ogni funzione Lambda. Puoi configurare un filtro di abbonamento per un gruppo di log per trasmetterne i log ad Amazon OpenSearch Service. Puoi configurare manualmente un filtro di abbonamento per ogni singolo gruppo di log che desideri trasmettere in streaming su Amazon OpenSearch Service. In alternativa, puoi implementare una soluzione che sottoscrive automaticamente nuovi gruppi di log ai ElasticSearch cluster. È possibile trasmettere i log a un ElasticSearch cluster nello stesso account o a un account centralizzato. Lo streaming dei log su un ElasticSearch cluster nello stesso account aiuta i proprietari dei carichi di lavoro ad analizzare e supportare meglio i propri carichi di lavoro.

Dovresti prendere in considerazione la possibilità di configurare un ElasticSearch cluster in un account centralizzato o condiviso per aggregare i log tra account, regioni e applicazioni. Ad esempio, AWS Control Tower configura un account Log Archive utilizzato per la registrazione centralizzata. Quando viene creato un nuovo account AWS Control Tower, i relativi AWS Config registri vengono inviati a un bucket S3 in questo account centralizzato. AWS CloudTrail La registrazione utilizzata da serve per la configurazione, le modifiche e AWS Control Tower la registrazione di controllo.

Per creare una soluzione centralizzata di analisi dei log delle applicazioni con Amazon OpenSearch Service, puoi distribuire uno o più cluster OpenSearch Amazon Service centralizzati sul tuo account di registrazione centralizzato e configurare gruppi di log negli altri account per trasmettere i log ai cluster centralizzati di Amazon Service. OpenSearch

Puoi creare cluster Amazon OpenSearch Service separati per gestire diverse applicazioni o livelli della tua architettura cloud che potrebbero essere distribuiti tra i tuoi account. L'utilizzo di cluster Amazon OpenSearch Service separati aiuta a ridurre i rischi di sicurezza e disponibilità e disporre di un cluster Amazon OpenSearch Service comune può semplificare la ricerca e la correlazione dei dati all'interno dello stesso cluster.

# Opzioni allarmanti con CloudWatch

L'esecuzione di un'analisi una tantum e automatizzata di metriche importanti consente di rilevare e risolvere i problemi prima che influiscano sui carichi di lavoro. CloudWatch semplifica la creazione di grafici e il confronto di più metriche utilizzando più statistiche in un periodo di tempo specifico. Puoi utilizzarlo CloudWatch per cercare tra tutte le metriche con i valori di dimensione richiesti per trovare le metriche necessarie per l'analisi.

Ti consigliamo di iniziare l'approccio di acquisizione delle metriche includendo un set iniziale di metriche e dimensioni da utilizzare come base per il monitoraggio di un carico di lavoro. Nel tempo, il carico di lavoro matura e puoi aggiungere metriche e dimensioni aggiuntive per aiutarti ad analizzarlo e supportarlo ulteriormente. Le tue applicazioni o i tuoi carichi di lavoro potrebbero utilizzare più AWS risorse e avere metriche personalizzate, dovresti raggruppare queste risorse in un namespace per facilitarne l'identificazione.

È inoltre necessario considerare in che modo i dati di registrazione e monitoraggio sono correlati in modo da poter identificare rapidamente i dati di registrazione e monitoraggio pertinenti per diagnosticare problemi specifici. È possibile utilizzare la mappa di AWS X-Ray traccia per correlare tracce, metriche, registri e allarmi per la diagnosi dei problemi. Dovresti anche prendere in considerazione l'inclusione di dimensioni aggiuntive nelle metriche e negli identificatori nei log per i tuoi carichi di lavoro per aiutarti a cercare e identificare rapidamente i problemi tra sistemi e servizi.

## Utilizzo degli allarmi per monitorare e CloudWatch avvisare

È possibile utilizzare gli CloudWatch allarmi per ridurre il monitoraggio manuale dei carichi di lavoro o delle applicazioni. Dovresti iniziare esaminando le metriche che stai acquisendo per ogni componente del carico di lavoro e determinare le soglie appropriate per ogni metrica. Assicurati di identificare quali membri del team devono essere avvisati quando viene superata una soglia. È necessario stabilire e indirizzare i gruppi di distribuzione, anziché i singoli membri del team.

CloudWatch gli allarmi possono integrarsi con la soluzione di gestione dei servizi per creare automaticamente nuovi ticket ed eseguire flussi di lavoro operativi. Ad esempio, AWS fornisce il AWS Service Management Connector per ServiceNowe per aiutarti AWS Service Management Connectora configurare rapidamente le integrazioni. Questo approccio è fondamentale per garantire che gli allarmi generati vengano riconosciuti e allineati ai flussi di lavoro operativi esistenti che potrebbero essere già definiti in questi prodotti.

Puoi anche creare più allarmi per la stessa metrica con soglie e periodi di valutazione diversi, il che aiuta a stabilire un processo di escalation. Ad esempio, se disponi di una `OrderQueueDepth` metrica che tiene traccia degli ordini dei clienti, potresti definire una soglia inferiore su un breve periodo medio di un minuto per avvisare i membri del team di applicazione tramite e-mail o Slack. Puoi anche definire un altro allarme per la stessa metrica per un periodo più lungo di 15 minuti alla stessa soglia e che invii pagine, invii e-mail e notifiche al team dell'applicazione e al responsabile del team dell'applicazione. Infine, è possibile definire un terzo allarme per una soglia media fissa su un periodo di 30 minuti che avvisi i dirigenti superiori e avvisi tutti i membri del team precedentemente informati. La creazione di più allarmi consente di intraprendere azioni diverse per condizioni diverse. Puoi iniziare con un semplice processo di notifica e poi modificarlo e migliorarlo secondo necessità.

## Utilizzo del rilevamento delle CloudWatch anomalie per il monitoraggio e l'allarme

Puoi utilizzare il rilevamento delle CloudWatch anomalie se non sei sicuro delle soglie da applicare per una particolare metrica o se desideri che un allarme regoli automaticamente i valori di soglia in base ai valori storici osservati. CloudWatch il rilevamento delle anomalie è particolarmente utile per le metriche che potrebbero comportare cambiamenti di attività regolari e prevedibili, ad esempio l'aumento degli ordini di acquisto giornalieri per la consegna in giornata prima di un orario limite. Il rilevamento delle anomalie abilita soglie che si adattano automaticamente e può aiutare a ridurre i falsi allarmi. Puoi abilitare il rilevamento delle anomalie per ogni metrica e statistica e configurare un allarme in base ai valori anomali. CloudWatch

Ad esempio, puoi abilitare il rilevamento delle anomalie per la `CPUUtilization` metrica e la statistica su un'istanza EC2. `AVG` Il rilevamento delle anomalie utilizza quindi fino a 14 giorni di dati storici per creare il modello di machine learning (ML). È possibile creare più allarmi con diverse bande di rilevamento delle anomalie per stabilire un processo di intensificazione degli allarmi, simile alla creazione di più allarmi standard con soglie diverse.

Per ulteriori informazioni su questa sezione, consulta Creazione di un CloudWatch allarme basato sul rilevamento delle anomalie nella documentazione. CloudWatch

## Allarmi in più regioni e account

I proprietari di applicazioni e carichi di lavoro devono creare allarmi a livello di applicazione per carichi di lavoro che si estendono su più regioni. Ti consigliamo di creare allarmi separati all'interno di ogni

account e regione in cui viene distribuito il carico di lavoro. Puoi semplificare e automatizzare questo processo utilizzando modelli e modelli indipendenti CloudFormation StackSets dall'account e dalla regione per distribuire risorse applicative con gli allarmi richiesti. ModelloÈ possibile configurare le azioni di allarme in modo che abbiano come target un argomento comune di Amazon Simple Notification Service (Amazon SNS), il che significa che viene utilizzata la stessa notifica o azione di riparazione indipendentemente dall'account o dalla regione.

In ambienti con più account e più regioni, ti consigliamo di creare allarmi aggregati per i tuoi account e le regioni per monitorare i problemi relativi agli account e alle regioni utilizzando CloudFormation StackSets e aggregare metriche, come la media di `CPUUtilization` tutte le istanze EC2.

Dovresti anche prendere in considerazione la creazione di allarmi standard per ogni carico di lavoro configurato per le metriche e i log standard che acquisisci. CloudWatch Ad esempio, puoi creare un allarme separato per ogni istanza EC2 che monitora la metrica di utilizzo della CPU e avvisa un team operativo centrale quando l'utilizzo medio della CPU supera l'80% su base giornaliera. Puoi anche creare un allarme standard che monitori l'utilizzo medio della CPU al di sotto del 10% su base giornaliera. Questi allarmi aiutano il team operativo centrale a collaborare con proprietari di carichi di lavoro specifici per modificare le dimensioni delle istanze EC2 quando necessario.

## Automatizzazione della creazione di allarmi con i tag delle istanze EC2

La creazione di un set standard di allarmi per le istanze EC2 può richiedere molto tempo, essere incoerente e soggetta a errori. Puoi accelerare il processo di creazione degli allarmi utilizzando la amazon-cloudwatch-auto-alarmssoluzione per creare automaticamente un set standard di CloudWatch allarmi per le tue istanze EC2 e creare allarmi personalizzati basati sui tag delle istanze EC2. La soluzione elimina la necessità di creare manualmente allarmi standard e può essere utile durante una migrazione su larga scala di istanze EC2 che utilizza strumenti come. CloudEndure Puoi anche implementare questa soluzione per supportare più regioni e CloudFormation StackSets account. Per ulteriori informazioni, consulta Usare i tag per creare e gestire CloudWatch allarmi Amazon per le istanze Amazon EC2 sul blog. AWS

# Monitoraggio della disponibilità di applicazioni e servizi

CloudWatch ti aiuta a monitorare e analizzare gli aspetti prestazionali e di runtime delle tue applicazioni e dei tuoi carichi di lavoro. È inoltre necessario monitorare gli aspetti di disponibilità e raggiungibilità delle applicazioni e dei carichi di lavoro. Puoi raggiungere questo obiettivo utilizzando un approccio di monitoraggio attivo con controlli di integrità di Amazon Route 53 e CloudWatch Synthetics.

Puoi utilizzare i controlli di integrità di Route 53 quando desideri monitorare la connettività a una pagina Web tramite HTTP o HTTPS o la connettività di rete tramite TCP verso un nome o un indirizzo IP pubblico del Domain Name System (DNS). I controlli di integrità di Route 53 avviano le connessioni dalle regioni specificate a intervalli di dieci o 30 secondi. Puoi scegliere più regioni in cui eseguire il controllo sanitario, ogni controllo sanitario viene eseguito in modo indipendente e devi scegliere almeno tre regioni. È possibile cercare nel corpo della risposta di una richiesta HTTP o HTTPS una sottostringa specifica se compare nei primi 5.120 byte di dati restituiti per la valutazione del controllo sanitario. Una richiesta HTTP o HTTPS è considerata integra se restituisce una risposta 2xx o 3xx. I controlli di integrità Route 53 possono essere utilizzati per creare un controllo di integrità composito controllando lo stato di altri controlli sanitari. È possibile eseguire questa operazione se si dispone di più endpoint di servizio e si desidera eseguire la stessa notifica quando uno di essi non funziona correttamente. Se utilizzi Route 53 per DNS, puoi configurare Route 53 in modo che esegua il failover su un'altra voce DNS nel caso in cui un controllo dello stato non funzioni correttamente. Per ogni carico di lavoro critico, dovresti prendere in considerazione la possibilità di configurare i controlli di integrità di Route 53 per gli endpoint esterni che sono fondamentali per le normali operazioni. I controlli di integrità di Route 53 possono aiutarti a evitare di scrivere la logica di failover nelle tue applicazioni.

CloudWatch synthetics consente di definire un canarino come script per valutare lo stato e la disponibilità dei carichi di lavoro. I Canaries sono script scritti in Node.js o Python e funzionano su protocolli HTTP o HTTPS. Creano funzioni Lambda nel tuo account che utilizzano Node.js o Python come framework. Ogni canarino che definisci può eseguire più chiamate HTTP o HTTPS verso endpoint diversi. Ciò significa che puoi monitorare lo stato di una serie di passaggi, come un caso d'uso o un endpoint con dipendenze a valle. Canaries crea CloudWatch metriche che includono ogni passaggio eseguito in modo da poter allarmare e misurare i diversi passaggi in modo indipendente. Sebbene i canarini richiedano una pianificazione e uno sforzo maggiori rispetto ai controlli sanitari della Route 53, offrono un approccio di monitoraggio e valutazione altamente personalizzabile. Le Canarie supportano anche risorse private in esecuzione all'interno del tuo cloud privato virtuale

(VPC), il che le rende ideali per il monitoraggio della disponibilità quando non disponi di un indirizzo IP pubblico per l'endpoint. Puoi anche usare canaries per monitorare i carichi di lavoro locali purché sia disponibile la connettività dall'interno del VPC all'endpoint. Ciò è particolarmente importante quando si dispone di un carico di lavoro che include endpoint esistenti in locale.

# Tracciamento delle applicazioni con AWS X-Ray

Una richiesta tramite la tua applicazione potrebbe consistere in chiamate a database, applicazioni e servizi Web in esecuzione su server locali, Amazon EC2, container o Lambda. Implementando il tracciamento delle applicazioni, è possibile identificare rapidamente la causa principale dei problemi nelle applicazioni che utilizzano componenti e servizi distribuiti. È possibile AWS X-Rayutilizzarlo per tracciare le richieste delle applicazioni su più componenti. X-Ray campiona e visualizza le richieste su un grafico di servizio quando fluiscono attraverso i componenti dell'applicazione e ogni componente è rappresentato come un segmento. X-Ray genera identificatori di traccia in modo da poter correlare una richiesta quando fluisce attraverso più componenti, il che consente di visualizzare la richiesta dall'inizio alla fine. È possibile migliorare ulteriormente questa funzionalità includendo annotazioni e metadati per aiutare a cercare e identificare in modo univoco le caratteristiche di una richiesta.

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

X-Ray fornisce un daemon X-Ray che puoi installare ed eseguire su Amazon EC2 e Amazon ECS per inoltrare i dati a X-Ray. X-Ray crea tracce per l'applicazione che acquisiscono dati sulle prestazioni dai server e dai contenitori che eseguono il daemon X-Ray che ha gestito la richiesta. X-Ray strumenta automaticamente le chiamate ai AWS servizi, come Amazon DynamoDB, come sottosegmenti mediante l'applicazione di patch all'SDK. AWS X-Ray può anche integrarsi automaticamente con le funzioni Lambda.

Se i componenti dell'applicazione effettuano chiamate a servizi esterni che non possono configurare e installare il demone X-Ray o lo strumento del codice, potete creare sottosegmenti per collegare le chiamate a servizi esterni. X-Ray mette in correlazione CloudWatch i log e le metriche con le tracce dell'applicazione se si utilizza il SDK AWS X-Ray per Java, il che significa che è possibile analizzare rapidamente le metriche e i log correlati per le richieste.

# Implementazione del demone X-Ray per tracciare applicazioni e servizi su Amazon EC2

È necessario installare ed eseguire il daemon X-Ray sulle istanze EC2 su cui vengono eseguiti i componenti dell'applicazione o i microservizi. Puoi utilizzare uno script di dati utente per distribuire il daemon X-Ray quando viene effettuato il provisioning delle istanze EC2 oppure puoi includerlo nel processo di creazione dell'AMI se crei le tue AMI. Ciò può essere particolarmente utile quando le istanze EC2 sono effimere.

È necessario utilizzare State Manager per garantire che il daemon X-Ray sia installato in modo coerente sulle istanze EC2. Per le istanze Windows di Amazon EC2, puoi utilizzare il RunPowerShellScript documento Systems Manager AWS- per eseguire lo script di Windows che scarica e installa l'agente X-Ray. Per le istanze EC2 su Linux, puoi utilizzare il RunShellScript documento AWS- per eseguire lo script Linux che scarica e installa l'agente come servizio.

È possibile utilizzare il RunRemoteScript documento Systems Manager AWS- per eseguire lo script in un ambiente multi-account. Devi creare un bucket S3 accessibile da tutti i tuoi account e, se lo utilizzi, ti consigliamo di creare un bucket S3 con una politica dei bucket basata sull'organizzazione. AWS Organizations Quindi carichi gli script nel bucket S3, ma assicurati che il ruolo IAM per le tue istanze EC2 sia autorizzato ad accedere al bucket e agli script.

Puoi anche configurare State Manager per associare gli script alle istanze EC2 su cui è installato l'agente X-Ray. Poiché tutte le istanze EC2 potrebbero non richiedere o utilizzare X-Ray, puoi indirizzare l'associazione con i tag delle istanze. Ad esempio, puoi creare l'associazione State Manager in base alla presenza di `InstallAWSXRayDaemonWindows` o tag. `InstallAWSXRayDaemonLinux`

# Implementazione del demone X-Ray per tracciare applicazioni e servizi su Amazon ECS o Amazon EKS

Puoi implementare il daemon X-Ray come contenitore secondario per carichi di lavoro basati su container come Amazon ECS o Amazon EKS. I contenitori delle applicazioni possono quindi connettersi al contenitore sidecar con collegamento ai contenitori se si utilizza Amazon ECS, oppure il contenitore può connettersi direttamente al contenitore sidecar su localhost se si utilizza la modalità di rete awsvpc.

Per Amazon EKS, puoi definire il demone X-Ray nella definizione del pod dell'applicazione e quindi l'applicazione può connettersi al daemon tramite localhost sulla porta container che hai specificato.

## Configurazione di Lambda per tracciare le richieste su X-Ray

L'applicazione potrebbe includere chiamate alle funzioni Lambda. Non è necessario installare il demone X-Ray per Lambda perché il processo daemon è completamente gestito da Lambda e non può essere configurato dall'utente. Puoi abilitarlo per la tua funzione Lambda utilizzando Console di gestione AWS e selezionando l'opzione Active Tracing nella console X-Ray.

Per ulteriore strumentazione, puoi abbinare l'X-Ray SDK alla funzione Lambda per registrare le chiamate in uscita e aggiungere annotazioni o metadati.

## Strumentazione delle vostre applicazioni per i raggi X

È necessario valutare l'SDK X-Ray che si allinea al linguaggio di programmazione dell'applicazione e classificare tutte le chiamate effettuate dall'applicazione verso altri sistemi. Esamina i client forniti dalla libreria che hai scelto e verifica se l'SDK è in grado di tracciare automaticamente la richiesta o la risposta dell'applicazione. Determina se i client forniti dall'SDK possono essere utilizzati per altri sistemi downstream. Per i sistemi esterni richiamati dall'applicazione e che non è possibile strumentare con X-Ray, è necessario creare sottosegmenti personalizzati per acquisirli e identificarli nelle informazioni di traccia.

Quando strumentate la vostra applicazione, assicuratevi di creare annotazioni per aiutarvi a identificare e cercare le richieste. Ad esempio, l'applicazione potrebbe utilizzare un identificatore per i clienti, ad esempio`customer id`, o segmentare utenti diversi in base al loro ruolo nell'applicazione.

È possibile creare un massimo di 50 annotazioni per ogni traccia, ma è possibile creare un oggetto di metadati contenente uno o più campi purché il documento del segmento non superi i 64 kilobyte. È consigliabile utilizzare le annotazioni in modo selettivo per individuare le informazioni e utilizzare l'oggetto di metadati per fornire un contesto più ampio che aiuti a risolvere i problemi della richiesta dopo che è stata individuata.

## Configurazione delle regole di campionamento a raggi X

Personalizzando le regole di campionamento, è possibile controllare la quantità di dati registrati e modificare il comportamento di campionamento senza modificare o ridistribuire il codice. Le

regole di campionamento indicano all'X-Ray SDK quante richieste registrare per una serie di criteri. Per impostazione predefinita, l'SDK X-Ray registra la prima richiesta ogni secondo e il cinque percento di eventuali richieste aggiuntive. Una richiesta al secondo è la riserva. In questo modo viene registrata almeno una traccia al secondo, purché il servizio soddisfi le richieste. Il cinque percento è la frequenza con cui vengono campionate le richieste aggiuntive oltre le dimensioni del serbatoio.

È necessario rivedere e aggiornare la configurazione predefinita per determinare un valore appropriato per l'account. I requisiti possono variare negli ambienti di sviluppo, test, test delle prestazioni e produzione. Potreste avere applicazioni che richiedono regole di campionamento proprie in base alla quantità di traffico che ricevono o al livello di criticità. È necessario iniziare con una linea di base e rivalutare regolarmente se la linea di base soddisfa i requisiti.

# Dashboard e visualizzazioni con CloudWatch

Le dashboard ti aiutano a concentrarti rapidamente sulle aree di interesse per le applicazioni e i carichi di lavoro. CloudWatchfornisce dashboard automatici e puoi anche creare facilmente dashboard che utilizzano metriche. CloudWatch CloudWatch le dashboard forniscono maggiori informazioni rispetto alla visualizzazione isolata delle metriche, perché consentono di correlare più metriche e identificare le tendenze. Ad esempio, una dashboard che include gli ordini ricevuti, la memoria, l'utilizzo della CPU e le connessioni al database può aiutarti a correlare le modifiche nelle metriche del carico di lavoro su più AWS risorse mentre il numero degli ordini aumenta o diminuisce.

È necessario creare dashboard a livello di account e applicazione per monitorare i carichi di lavoro e le applicazioni. Puoi iniziare utilizzando i dashboard CloudWatch automatici, che sono dashboard a livello di servizio preconfigurati con metriche specifiche del AWS servizio. Le dashboard di servizio automatiche mostrano tutte le metriche standard del servizio. CloudWatch I dashboard automatici rappresentano graficamente tutte le risorse utilizzate per ogni metrica del servizio e ti aiutano a identificare rapidamente le risorse anomale nel tuo account. Questo può aiutarti a identificare le risorse con un utilizzo elevato e basso, il che può aiutarti a ottimizzare i costi.

## Creazione di dashboard multiservizio

È possibile creare dashboard interservizi visualizzando la dashboard automatica a livello di servizio per un AWS servizio e utilizzando l'opzione Aggiungi alla dashboard dal menu Azioni. Puoi quindi aggiungere metriche da altre dashboard automatiche alla tua nuova dashboard e rimuovere le metriche per restringere l'attenzione della dashboard. Dovresti anche aggiungere metriche personalizzate per tenere traccia delle osservazioni chiave (ad esempio, ordini ricevuti o transazioni al secondo). La creazione di una dashboard multiservizio personalizzata ti aiuta a concentrarti sulle metriche più pertinenti per il tuo carico di lavoro. Ti consigliamo di creare dashboard multiservizio a livello di account che coprano le metriche chiave e mostrino tutti i carichi di lavoro di un account.

Se disponi di uno spazio ufficio centrale o di un'area comune per i tuoi team operativi sul cloud, puoi visualizzare la CloudWatch dashboard su un grande monitor TV in modalità a schermo intero con aggiornamento automatico.

## Creazione di dashboard specifici per applicazioni o carichi di lavoro

Ti consigliamo di creare dashboard specifici per applicazioni e carichi di lavoro incentrati su metriche e risorse chiave per ogni applicazione o carico di lavoro critico nell'ambiente di produzione. Le

dashboard specifiche per applicazioni e carichi di lavoro si concentrano sulle metriche personalizzate dell'applicazione o del carico di lavoro e su importanti metriche delle risorse che ne influenzano le prestazioni. AWS

È necessario valutare e personalizzare regolarmente le dashboard dell' CloudWatch applicazione o del carico di lavoro per tenere traccia delle metriche chiave dopo che si sono verificati gli incidenti. È inoltre necessario aggiornare i dashboard specifici dell'applicazione o del carico di lavoro quando le funzionalità vengono introdotte o ritirate. Gli aggiornamenti ai dashboard specifici per carichi di lavoro e applicazioni dovrebbero essere un'attività necessaria per il miglioramento continuo della qualità, oltre alla registrazione e al monitoraggio.

## Creazione di dashboard per più account o più regioni

AWS le risorse sono principalmente regionali e le metriche, gli allarmi e i dashboard sono specifici della regione in cui vengono distribuite le risorse. Ciò può richiedere la modifica delle regioni per visualizzare metriche, dashboard e allarmi per carichi di lavoro e applicazioni interregionali. Se separi le applicazioni e i carichi di lavoro in più account, ti potrebbe anche essere richiesto di autenticarti nuovamente e accedere a ciascun account. Tuttavia, CloudWatch supporta la visualizzazione dei dati tra account e regioni diverse da un unico account, il che significa che puoi visualizzare metriche, allarmi, dashboard e widget di registro in un unico account e regione. Ciò è molto utile se si dispone di un account di registrazione e monitoraggio centralizzato.

I proprietari degli account e i proprietari dei team applicativi devono creare dashboard per applicazioni specifiche dell'account e distribuite in più regioni, per monitorare efficacemente le metriche chiave in una posizione centralizzata. CloudWatchLe dashboard supportano automaticamente i widget interregionali, il che significa che puoi creare una dashboard che includa metriche provenienti da più regioni senza ulteriori configurazioni.

Un'eccezione importante è il widget CloudWatch Logs Insights, poiché i dati di registro possono essere visualizzati solo per l'account e la regione a cui si è attualmente connessi. Puoi creare metriche specifiche per regione dai tuoi log utilizzando filtri metrici e queste metriche possono essere visualizzate in una dashboard interregionale. È quindi possibile passare alla regione specifica quando è necessario analizzare ulteriormente tali registri.

I team operativi dovrebbero creare dashboard centralizzate che monitorino importanti metriche tra account e aree geografiche. Ad esempio, puoi creare una dashboard per più account che includa l'utilizzo aggregato della CPU in ogni account e regione. Puoi anche utilizzare la matematica metrica per aggregare e gestire i dati su più account e regioni.

# Utilizzo della matematica metrica per ottimizzare l'osservabilità e l'allarme

Puoi usare la matematica metrica per aiutare a calcolare le metriche in formati ed espressioni pertinenti per i tuoi carichi di lavoro. Le metriche calcolate possono essere salvate e visualizzate su una dashboard a scopo di tracciamento. Ad esempio, i parametri di volume standard di Amazon EBS forniscono il numero di operazioni di lettura (`VolumeReadOps`) e scrittura (`VolumeWriteOps`) eseguite in un periodo specifico.

Tuttavia, AWS fornisce linee guida sulle prestazioni dei volumi di Amazon EBS in IOPS. Puoi rappresentare graficamente e calcolare gli IOPS per il tuo volume Amazon EBS in termini matematici metrici aggiungendo `VolumeReadOps` `VolumeWriteOps` e dividendo per il periodo scelto per questi parametri.

In questo esempio, sommiamo gli IOPS nel periodo e poi dividiamo per la durata del periodo per ottenere gli IOPS. È quindi possibile impostare un allarme in base a questa espressione matematica metrica per avvisare l'utente quando l'IOPS del volume si avvicina alla capacità massima per il tipo di volume corrispondente. Per ulteriori informazioni ed esempi sull'utilizzo della matematica metrica per monitorare i file system Amazon Elastic File System (Amazon EFS) con CloudWatch metriche, consulta Amazon CloudWatch Metric Math semplifica il monitoraggio quasi in tempo reale dei file system Amazon EFS e altro sul blog. AWS

# Utilizzo di dashboard automatici per Amazon ECS, Amazon EKS e Lambda con Insights e Lambda Insights CloudWatchContainer CloudWatch

CloudWatch Container Insights crea dashboard dinamici e automatici per i carichi di lavoro dei container in esecuzione su Amazon ECS e Amazon EKS. È necessario consentire a Container Insights di avere la visibilità di CPU, memoria, disco, rete e informazioni diagnostiche come gli errori di riavvio dei contenitori. Container Insights genera dashboard dinamici che è possibile filtrare rapidamente a livello di cluster, istanza o nodo del contenitore, servizio, attività, pod e singolo contenitore. Container Insights è configurato a livello di cluster e nodo o istanza di contenitore a seconda del AWS servizio.

Analogamente a Container Insights, CloudWatch Lambda Insights crea dashboard dinamici e automatici per le funzioni Lambda. Questa soluzione raccoglie, aggrega e riepiloga le metriche a

livello di sistema, tra cui tempo di CPU, memoria, disco e rete. Inoltre, raccoglie, aggrega e riepiloga informazioni diagnostiche come partenze a freddo e arresti degli operatori Lambda per aiutarti a isolare e risolvere rapidamente i problemi relativi alle funzioni Lambda. Lambda è abilitata a livello di funzione e non richiede alcun agente.

Container Insights e Lambda Insights consentono inoltre di passare rapidamente ai registri delle applicazioni o delle prestazioni, alle tracce X-Ray e a una mappa dei servizi per visualizzare i carichi di lavoro dei container. Entrambi utilizzano il formato metrico CloudWatch incorporato per acquisire metriche e registri delle prestazioni. CloudWatch

Puoi creare una CloudWatch dashboard condivisa per il tuo carico di lavoro che utilizza le metriche acquisite da Container Insights e Lambda Insights. Puoi farlo filtrando e visualizzando la dashboard automatica tramite CloudWatch Container Insights e quindi scegliendo l'opzione Aggiungi a Dashboard che consente di aggiungere le metriche visualizzate a una dashboard standard. CloudWatch Puoi quindi rimuovere o personalizzare le metriche e aggiungere altre metriche per rappresentare correttamente il tuo carico di lavoro.

# CloudWatch integrazione con AWS i servizi

AWS fornisce molti servizi che includono opzioni di configurazione aggiuntive per la registrazione e le metriche. Questi servizi spesso consentono di configurare i log per l'output CloudWatch dei log e le metriche per l'output CloudWatch delle metriche. L'infrastruttura sottostante utilizzata per fornire questi servizi è gestita da AWS ed è inaccessibile, ma è possibile utilizzare le opzioni di registrazione e metrica dei servizi forniti per ottenere ulteriori informazioni e risolvere i problemi. Ad esempio, puoi pubblicare i log di flusso VPC su CloudWatch, oppure puoi anche configurare istanze di Amazon Relational Database Service (Amazon RDS) su cui pubblicare i log. CloudWatch

La maggior parte dei AWS servizi registra le proprie chiamate API con integrazione in. AWS CloudTrail CloudTrail supporta anche l'integrazione con CloudWatch Logs, il che significa che è possibile cercare e analizzare l'attività nei AWS servizi. Puoi anche utilizzare o Amazon EventBridge per creare e configurare automazione e notifiche con regole di evento per azioni specifiche eseguite nei AWS servizi. Alcuni servizi si integrano direttamente con EventBridge. Puoi anche creare eventi organizzati tramite CloudTrail.

# Amazon Managed Grafana per dashboard e visualizzazione

Amazon Managed Grafana può essere usato per osservare e visualizzare i carichi di lavoro. AWS Amazon Managed Grafana ti aiuta a visualizzare e analizzare i tuoi dati operativi su larga scala. Grafana è una piattaforma di analisi open source che ti aiuta a interrogare, visualizzare, avvisare e comprendere le tue metriche ovunque siano archiviate. Amazon Managed Grafana è particolarmente utile se la tua organizzazione utilizza già Grafana per la visualizzazione dei carichi di lavoro esistenti e desideri estendere la copertura ai carichi di lavoro. AWS Puoi usare Amazon Managed Grafana CloudWatch aggiungendolo come fonte di dati, il che significa che puoi creare visualizzazioni utilizzando metriche. CloudWatch Amazon Managed Grafana supporta AWS Organizations e puoi centralizzare i dashboard utilizzando i CloudWatch parametri di più account e regioni.

La tabella seguente fornisce i vantaggi e le considerazioni per l'utilizzo di Amazon Managed Grafana CloudWatch anziché per il dashboard. Un approccio ibrido potrebbe essere adatto in base ai diversi requisiti degli utenti finali, dei carichi di lavoro e delle applicazioni.

| | |
|---|---|
| Crea visualizzazioni e dashboard che si integrano con le fonti di dati supportate da Amazon Managed Grafana e Grafana open source | Amazon Managed Grafana ti aiuta a creare visualizzazioni e dashboard da molte fonti di dati diverse, incluse le metriche. CloudWatch Amazon Managed Grafana include una serie di fonti di dati integrate che comprendono AWS servizi, software open source e software COTS. Per ulteriori informazioni su questo argomento, consulta Sorgenti dati integrate nella documentazione di Amazon Managed Grafana. Puoi anche aggiungere il supporto per più fonti di dati aggiornando il tuo spazio di lavoro a Grafana Enterprise. Grafana supporta anche plugin di sorgenti dati che consenton o di comunicare con diversi sistemi esterni. CloudWatch I dashboard richiedono una CloudWatch metrica o una query di CloudWatc h Logs Insights per visualizzare i dati su una dashboard. CloudWatch |

| | |
|---|---|
| Gestisci l'accesso alla tua soluzione di dashboard separatamente dall'accesso all'account AWS | Amazon Managed Grafana richiede l'uso di AWS IAM Identity Center (IAM Identity Center) e AWS Organizations per l'autenticazione e l'autorizzazione. Ciò ti consente di autentica re gli utenti su Grafana utilizzando la federazio ne delle identità che potresti già utilizzare con IAM Identity Center o. AWS Organizations Tuttavia, se non utilizzi IAM Identity Center oppure AWS Organizations, è configurato come parte del processo di configurazione di Amazon Managed Grafana. Questo potrebbe diventare un problema se la tua organizzazione ha limitato l'uso di IAM Identity Center o AWS Organizations. |
| Acquisisci e accedi ai dati su più account e regioni con integrazione AWS Organizations | Amazon Managed Grafana si integra con AWS Organizations per consentirti di leggere dati da AWS fonti come CloudWatch Amazon OpenSearch Service su tutti i tuoi account. In questo modo è possibile creare dashboard che mostrano visualizzazioni utilizzando i dati di tutti i tuoi account. Per abilitare automatic amente l'accesso ai dati AWS Organizations, devi configurare l'area di lavoro Amazon Managed Grafana nell' AWS Organizations account di gestione. Questa operazione non è consigliata in base alle AWS Organizat ions best practice per l'account di gestione. Al contrario, supporta CloudWatch anche dashboard per le metriche tra account e aree geografiche diverse. CloudWatch |

| | |
|---|---|
| Usa widget di visualizzazione avanzati e definizioni Grafana disponibili nella community open source | Grafana offre un'ampia raccolta di visualizz azioni che puoi utilizzare per creare i tuoi dashboard. È disponibile anche un'ampia libreria di dashboard fornite dalla community che puoi modificare e riutilizzare in base alle tue esigenze. |
| Usa i dashboard con le implementazioni Grafana nuove ed esistenti | Se utilizzi già Grafana, puoi importare ed esportare dashboard dalle tue distribuzioni Grafana e personalizzarle per l'uso in Amazon Managed Grafana. Amazon Managed Grafana ti consente di standardizzare Grafana come soluzione di dashboard. |
| Configurazione e configurazione avanzate per aree di lavoro, autorizzazioni e fonti di dati | Amazon Managed Grafana ti consente di creare più aree di lavoro Grafana con un proprio set di origini dati, utenti e policy configurati. Questo può aiutarti a soddisfar e requisiti di casi d'uso più avanzati, nonché configurazioni di sicurezza avanzate. Le funzionalità avanzate potrebbero richiedere ai tuoi team di accrescere la loro esperienza con Grafana se non dispongono già di queste competenze. |

# Progettazione e implementazione della registrazione e del monitoraggio con CloudWatch le domande frequenti

Questa sezione fornisce le risposte alle domande più frequenti sulla progettazione e implementazione di una soluzione di registrazione e monitoraggio con. CloudWatch

## Dove posso archiviare i miei file CloudWatch di configurazione?

L' CloudWatch agente per Amazon EC2 può applicare più file di configurazione archiviati nella directory di CloudWatch configurazione. Idealmente, dovresti archiviare la CloudWatch configurazione come un set di file perché puoi controllare la versione e riutilizzarla su più account e ambienti. Per ulteriori informazioni su questo argomento, consulta la Gestione delle configurazioni CloudWatch sezione di questa guida. In alternativa, puoi archiviare i file di configurazione in un repository attivo GitHub e automatizzare il recupero dei file di configurazione quando viene fornita una nuova istanza EC2.

## Come posso creare un ticket nella mia soluzione di gestione dei servizi quando viene generato un allarme?

Integri il tuo sistema di gestione dei servizi con un argomento Amazon Simple Notification Service (Amazon SNS) e configuri CloudWatch l'allarme per notificare l'argomento SNS quando viene generato un allarme. Il tuo sistema integrato riceve il messaggio SNS e può creare un ticket utilizzando i tuoi sistemi di gestione dei servizi oppure. APIs SDKs

## Come posso CloudWatch utilizzarlo per acquisire i file di registro nei miei contenitori?

Le attività di Amazon ECS e i pod Amazon EKS possono essere configurati per inviare automaticamente l'output STDOUT e STDERR a. CloudWatch L'approccio consigliato per la registrazione delle applicazioni containerizzate consiste nell'inviare l'output ai container a STDOUT e STDERR. Questo è trattato anche nel manifesto dell'app Twelve-Factor.

Tuttavia, se desideri inviare file di log specifici a, CloudWatch puoi montare un volume nel tuo pod Amazon EKS o nella definizione di attività Amazon ECS su cui l'applicazione scriverà i suoi file di

lotto e utilizzare un contenitore laterale per Fluentd o Fluent Bit a cui inviare i log. CloudWatch È consigliabile prendere in considerazione il collegamento simbolico di un file di registro specifico nel contenitore a e. `/dev/stdout` `/dev/stderr` Per ulteriori informazioni su questo argomento, consulta Visualizza i registri per un contenitore o un servizio nella documentazione Docker.

## Come posso monitorare i problemi di salute dei servizi? AWS

È possibile utilizzare il Dashboard AWS Healthper monitorare gli eventi AWS sanitari. È inoltre possibile fare riferimento al aws-health-tools GitHub repository per esempi di soluzioni di automazione relative agli eventi AWS sanitari.

## Come posso creare una CloudWatch metrica personalizzata quando non esiste il supporto degli agenti?

Puoi utilizzare il formato metrico incorporato in cui inserire le metriche. CloudWatch Puoi anche utilizzare AWS SDK (ad esempio, put_metric_data), AWS CLI (ad esempio) o AWS API (ad esempio put-metric-data) per creare metriche personalizzate. PutMetricData Dovresti considerare in che modo qualsiasi logica personalizzata verrà mantenuta a lungo termine. Un approccio potrebbe essere quello di utilizzare Lambda con il supporto integrato del formato metrico incorporato per creare le metriche, insieme a una regola di pianificazione CloudWatch degli eventi per stabilire il periodo per la metrica.

## Come posso integrare i miei strumenti di registrazione e monitoraggio esistenti con? AWS

È necessario fare riferimento alle linee guida fornite dal fornitore del software o del servizio per l'integrazione con. AWS Potresti essere in grado di utilizzare il software dell'agente, l'SDK o un'API fornita per inviare log e metriche alla loro soluzione. Potresti anche essere in grado di utilizzare una soluzione open source, come Fluentd o Fluent Bit, configurata secondo le specifiche del fornitore. Puoi anche utilizzare i filtri di abbonamento AWS SDK e CloudWatch Logs con Lambda e Kinesis Data Streams per creare processori di log e shipper personalizzati. Infine, dovresti considerare anche come integrerai il software se utilizzi più account e regioni.

# Resources

## Introduzione

- AWS Well-Architected

## Obiettivi aziendali specifici

- logging-monitoring-apg-guide-esempi
- Sei vantaggi del cloud computing

## Pianificazione dell' CloudWatch implementazione

- AWS Organizations terminology and concepts
- AWS Systems Manager Configurazione rapida
- Raccolta di parametri e log dalle istanze Amazon EC2 e dai server locali con l'agente CloudWatch
- cloudwatch-config-s3-bucket.yaml
- Crea il file di configurazione dell'agente con la procedura guidata CloudWatch
- Enterprise DevOps: perché dovresti eseguire ciò che costruisci
- Exporting log data to Amazon S3
- Controllo granulare degli accessi in Amazon Service OpenSearch
- Quote Lambda
- Crea o modifica manualmente il file di configurazione dell' CloudWatch agente
- Elaborazione in tempo reale dei dati di registro con abbonamenti
- Strumenti su cui basarsi AWS

## Configurazione dell' CloudWatch agente per le istanze EC2 e i server locali

- Dimensioni metriche di Amazon EC2

- Istanze con prestazioni stabili
- CloudWatch set di metriche predefiniti per agenti
- Raccogli le metriche di processo con il plugin procstat
- Configurazione dell'agente per procstat CloudWatch
- Gestisci il monitoraggio dettagliato delle tue istanze EC2
- Acquisizione di log ad alta cardinalità e generazione di metriche con formato metrico incorporato CloudWatch
- Lavorare con gruppi di log e flussi di log
- Elenca le CloudWatch metriche disponibili per le tue istanze
- PutLogEvents
- Recupera metriche personalizzate con collectd
- Recupera metriche personalizzate con StatSD

## CloudWatch approcci di installazione di agenti per Amazon EC2 e server locali

- Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud
- Crea un'attivazione a istanza gestita per un ambiente ibrido
- Crea ruoli e utenti IAM da utilizzare con l'agente CloudWatch
- Scarica e configura l' CloudWatch agente utilizzando la riga di comando
- Come posso configurare i server locali che utilizzano l'agente Systems Manager e l'agente unificato per utilizzare solo CloudWatch credenziali temporanee?
- Prerequisiti per le operazioni relative ai set di stack
- Utilizzo di istanze spot

## Registrazione e monitoraggio su Amazon ECS

- amazon-cloudwatch-logs-for-bit fluente
- Metriche di Amazon ECS CloudWatch
- Parametri di Amazon ECS Container Insights
- Agente container Amazon ECS

- Tipi di lancio di Amazon ECS
- Implementazione dell' CloudWatch agente per raccogliere parametri a livello di istanza EC2 su Amazon ECS
- ecs_cluster_with_cloudwatch_linux.yaml
- esempio ecs_cw_emf_
- esempio ecs_firelense_emf
- ecs-task-nginx-firelense.json
- Recupero di metadati AMI ottimizzati per Amazon ECS
- Utilizzo del driver di registro awslogs
- Utilizzo delle librerie client per generare log in formato metrico incorporato

## Registrazione e monitoraggio su Amazon EKS

- Registrazione del piano di controllo Amazon EKS
- amazon_eks_managed_node_group_launch_config.yaml
- Nodi Amazon EKS
- amazon-eks-nodegroup.yaml
- Contratto sul livello di servizio Amazon EKS
- Monitoraggio delle metriche di Container Insights Prometheus
- Controlla le metriche del piano con Prometheus
- Registrazione Fargate
- Fluent Bit per Amazon EKS su Fargate
- Come acquisire i log delle applicazioni quando si utilizza Amazon EKS su Fargate
- Installazione dell' CloudWatch agente per raccogliere le metriche di Prometheus
- Installazione del server Kubernetes Metrics
- kubernetes/dashboard
- Kubernetes Horizontal Pod Autoscaler
- Componenti Kubernetes Control Plane
- pod Kubernetes
- Supporto per i modelli di avvio
- Gruppi di nodi gestiti

- Comportamento dell'aggiornamento del nodo gestito
- metrics-server
- Monitoraggio di Amazon EKS su Fargate con Prometheus e Grafana
- prometheus_jmx
- prometeo/jmx_exporter
- Raccolta di sorgenti Prometheus aggiuntive e importazione di tali metriche
- Nodi autogestiti
- Invia log a Logs CloudWatch
- Configura FluentD per inviare i log ai DaemonSet Logs CloudWatch
- Configura un carico Java/JMX di lavoro di esempio su Amazon EKS e Kubernetes
- Tutorial per aggiungere un nuovo target di scrape Prometheus: metriche del Prometheus API Server
- Vertical Pod Autoscaler

## Registrazione e metriche per AWS Lambda

- Errori di invocazione Lambda
- logging — Funzione di registrazione per Python
- Utilizzo delle librerie client per generare log in formato metrico incorporato
- Utilizzo delle metriche delle funzioni Lambda

## Ricerca e analisi dei log in CloudWatch

- La famiglia Beats
- Logstash elastico
- Pila elastica
- Streaming CloudWatch registra i dati su Amazon Service OpenSearch

## Opzioni allarmanti con CloudWatch

- amazon-cloudwatch-auto-alarms

- AWS Connettore di gestione dei servizi per Jira Service Management Cloud
- AWS Connettore di gestione dei servizi per Jira Service Management Data Center
- AWS Connettore di gestione dei servizi per ServiceNow

## Monitoraggio della disponibilità di applicazioni e servizi

- Configurazione di un failover DNS

## Tracciamento delle applicazioni con AWS X-Ray

- Rete di attività Amazon ECS
- Configuring sampling rules in the X-Ray console (Configurazione delle regole di campionamento nella console X-Ray)
- Esegui PowerShell comandi o script di Windows
- Esecuzione del daemon X-Ray su Amazon EC2
- Invio di dati di traccia a X-Ray
- Grafico di servizio in X-Ray

## Dashboard e visualizzazioni con CloudWatch

- Amazon CloudWatch Metric Math semplifica il monitoraggio quasi in tempo reale dei file system Amazon EFS
- Configurazione di Container Insights CloudWatch
- Utilizzo della matematica metrica

## CloudWatch integrazione con i servizi AWS

- AWS CloudTrail servizi e integrazioni supportati
- Eventi da Servizi AWS Amazon EventBridge
- Eventi del servizio AWS forniti tramite AWS CloudTrail
- Monitoraggio dei file di CloudTrail registro con CloudWatch Logs

- Pubblicazione dei log del database su Logs CloudWatch
- Pubblicazione dei log di flusso in Logs CloudWatch

## Amazon Managed Grafana per dashboard e visualizzazione

- Le migliori pratiche per l'account di gestione in AWS Organizations
- Fonti di dati integrate per Amazon Managed Grafana
- Dashboard tra account e regioni diverse in CloudWatch
- Plugin Grafana

# 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 di registrazione aggiornate | È stata aggiornata la sezione sulla registrazione di. AWS Lambda | 17 aprile 2023 |
| Informazioni di configurazione aggiornate | È stata aggiornata e rinominat a la sezione relativa alla creazione e all'archiviazione delle CloudWatch configura zioni. | 9 febbraio 2023 |
| Informazioni aggiornate sulle metriche | Sono state aggiornate le informazioni sui parametri delle applicazioni personali zzate nella sezione Metrics for Amazon ECS. | 31 gennaio 2023 |
| Avvisi di anteprima rimossi | Amazon Managed Grafana è generalmente disponibile. | 25 maggio 2022 |
| Sezione rimossa | CloudWatch SDK Metrics non è più supportato. | 7 gennaio 2022 |
| Pubblicazione iniziale | — | 30 aprile 2021 |

# AWS Glossario delle linee guida prescrittive

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

## Numeri

7 R

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

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

# A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione di aggregazione

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

# B

bot difettoso

Un bot che ha lo scopo di interrompere o causare danni a individui o organizzazioni.

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

implementazione blu/verde

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

bot

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

botnet

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

ramo

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

accesso break-glass

In circostanze eccezionali e tramite una procedura approvata, un mezzo rapido per consentire a un utente di accedere a un sito a Account AWS cui in genere non dispone delle autorizzazioni necessarie. Per ulteriori informazioni, vedere l'indicatore Implementate break-glass procedures nella guida Well-Architected AWS .

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

# C

CAF

Vedi Cloud Adoption AWS Framework.

implementazione canaria

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

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

Queste fasi sono state definite da Stephen Orban nel post sul blog The Journey Toward Cloud-First & the Stages of Adoption on the Enterprise Strategy. Cloud AWS Per informazioni su come si relazionano alla strategia di AWS migrazione, consulta la guida alla preparazione alla migrazione.

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

integrazione e distribuzione continua (continuous integration and continuous delivery, CI/CD)

Il processo di automazione delle fasi di origine, compilazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD viene comunemente descritto come una pipeline. CI/CD può aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le consegne. Per ulteriori informazioni, consulta Vantaggi

della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

CV

Vedi visione artificiale.

# D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di

mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro,Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Per informazioni su come utilizzare la progettazione basata sul dominio con il modello del fico strangolatore (Strangler Fig), consulta la sezione Modernizzazione incrementale dei servizi Web Microsoft ASP.NET (ASMX) legacy utilizzando container e il Gateway Amazon API.

DOTT.

Vedi disaster recovery.

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, è possibile AWS CloudFormation utilizzarlo per rilevare deviazioni nelle risorse di sistema oppure AWS Control Tower per rilevare cambiamenti nella landing zone che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

# E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. I sistemi big-endian memorizzano per primo il byte più importante. I sistemi little-endian memorizzano per primo il byte meno importante.

endpoint

Vedi service endpoint.

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.
- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.

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

epica

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

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

# F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi modello di base.

modello di fondazione (FM)

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

# G

IA generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

In Amazon CloudFront, un'opzione per impedire agli utenti di determinati paesi di accedere alle distribuzioni di contenuti. Puoi utilizzare un elenco consentito o un elenco di blocco per specificare i paesi approvati e vietati. Per ulteriori informazioni, consulta Limitare la distribuzione geografica dei contenuti nella CloudFront documentazione.

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

# H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in

genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. AWS offre AWS SCT che aiuta con le conversioni dello schema.

alta disponibilità (HA)

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

modernizzazione storica

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

dati di blocco

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

Subito dopo la conversione, il periodo di tempo in cui un team di migrazione gestisce e monitora le applicazioni migrate nel cloud per risolvere eventuali problemi. In genere, questo periodo dura

da 1 a 4 giorni. Al termine del periodo di hypercare, il team addetto alla migrazione in genere trasferisce la responsabilità delle applicazioni al team addetto alle operazioni cloud.

# I

IaC

Vedi l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

In un'architettura AWS multi-account, un VPC che accetta, ispeziona e indirizza le connessioni di rete dall'esterno di un'applicazione. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

Una strategia di conversione in cui si esegue la migrazione dell'applicazione in piccole parti anziché eseguire una conversione singola e completa. Ad esempio, inizialmente potresti spostare

solo alcuni microservizi o utenti nel nuovo sistema. Dopo aver verificato che tutto funzioni correttamente, puoi spostare in modo incrementale microservizi o utenti aggiuntivi fino alla disattivazione del sistema legacy. Questa strategia riduce i rischi associati alle migrazioni di grandi dimensioni.

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

# L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

Una landing zone è un AWS ambiente multi-account ben progettato, scalabile e sicuro. Questo è un punto di partenza dal quale le organizzazioni possono avviare e distribuire rapidamente carichi di lavoro e applicazioni con fiducia nel loro ambiente di sicurezza e infrastruttura. Per ulteriori

informazioni sulle zone di destinazione, consulta la sezione Configurazione di un ambiente AWS multi-account sicuro e scalabile.

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

Un sistema che memorizza per primo il byte meno importante. Vedi anche endianità.

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

# M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati

dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione Machine learning.

ramo principale

Vedi filiale.

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

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

migrazione su larga scala

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

fabbrica di migrazione

Team interfunzionali che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory includono in genere operazioni, analisti e

proprietari aziendali, ingegneri addetti alla migrazione, sviluppatori e DevOps professionisti che lavorano nell'ambito degli sprint. Tra il 20% e il 50% di un portfolio di applicazioni aziendali è costituito da schemi ripetuti che possono essere ottimizzati con un approccio di fabbrica. Per ulteriori informazioni, consulta la discussione sulle fabbriche di migrazione e la Guida alla fabbrica di migrazione al cloud in questo set di contenuti.

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

# O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

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

gestione del cambiamento organizzativo (OCM)

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

persone, a causa della velocità di cambiamento richiesta nei progetti di adozione del cloud. Per ulteriori informazioni, consultare la Guida OCM.

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

Vedi la revisione della prontezza operativa.

NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

In un'architettura AWS multi-account, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

# P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

# Q

Piano di query

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

regressione del piano di query

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

# R

Matrice RACI

Vedi responsabile, responsabile, consultato, informato (RACI).

RAG

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

Vedi responsabile, responsabile, consultato, informato (RACI).

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Region

Una raccolta di AWS risorse in un'area geografica. Ciascuna Regione AWS è isolata e indipendente dalle altre per fornire tolleranza agli errori, stabilità e resilienza. Per ulteriori informazioni, consulta Specificare cosa può 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 alle interruzioni o di ripristinarle. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud AWSPer ulteriori informazioni, vedere Cloud AWS Resilience.

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi obiettivo del punto di ripristino.

VERSO

Vedi obiettivo del tempo di ripristino.

runbook

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

# S

SAML 2.0

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

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

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

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

Una politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta le politiche di controllo del servizio nella AWS Organizations documentazione.

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

Vedi il sistema di gestione delle informazioni e degli eventi sulla sicurezza.

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

# T

tag

Coppie chiave-valore che fungono da metadati per l'organizzazione delle risorse. AWS Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse. Per ulteriori informazioni, consulta Tagging delle risorse AWS.

variabile di destinazione

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

elenco di attività

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

ambiente di test

Vedi ambiente.

training

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

Transit Gateway

Un hub di transito di rete che puoi utilizzare per interconnettere le tue reti VPCs e quelle locali. Per ulteriori informazioni, consulta Cos'è un gateway di transito nella AWS Transit Gateway documentazione.

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

# U

incertezza

Un concetto che si riferisce a informazioni imprecise, incomplete o sconosciute che possono minare l'affidabilità dei modelli di machine learning predittivi. Esistono due tipi di incertezza: l'incertezza epistemica, che è causata da dati limitati e incompleti, mentre l'incertezza aleatoria è causata dal rumore e dalla casualità insiti nei dati. Per ulteriori informazioni, consulta la guida Quantificazione dell'incertezza nei sistemi di deep learning.

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

# V

vacuum

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

controllo delle versioni

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

Peering VPC

Una connessione tra due VPCs che consente di indirizzare il traffico utilizzando indirizzi IP privati. Per ulteriori informazioni, consulta Che cos'è il peering VPC? nella documentazione di Amazon VPC.

vulnerabilità

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

# W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

# Z

exploit zero-day

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

vulnerabilità zero-day

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

prompt zero-shot

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

applicazione zombie

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

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