Progettazione e implementazione della registrazione e del monitoraggio con Amazon CloudWatch

AWS Guida prescrittiva

AWS Guida prescrittiva: Progettazione e implementazione della registrazione e del 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, DevOps agli ingegneri e agli ingegneri delle applicazioni che gestiscono i carichi di lavoro sulAWS cloud.

Il tuo approccio di registrazione e monitoraggio dovrebbe basarsi sui sei pilastri delAWS Well-Architected 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 aiutandoti ad analizzare e regolare in modo proattivo la tua infrastruttura.

Questa guida non tratta in modo approfondito la registrazione e il monitoraggio per la sicurezza o l'ottimizzazione dei costi perché si tratta di argomenti che richiedono una valutazione approfondita. Esistono moltiAWS servizi che supportano la registrazione e il monitoraggio della sicurezza AWS CloudTrailAWS Config, tra cui Amazon Inspector, Amazon Detective, Amazon Macie GuardDuty, Amazon e AWS Security Hub. Puoi anche utilizzare i AWS Cost ExplorerAWSbudget e le metriche diCloudWatch fatturazione per l'ottimizzazione dei costi.

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

Acquisizione e inserimento di file di registro e metriche	Identifica, configura e invia i log e le metriche di sistema e delle applicazioni aAWS servizi da fonti diverse.
Ricerca e analisi dei registri	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 degli 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 relativi ai 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 analisi delle cause principali e risolvere i problemi.
Creazione di dashboard e visualizzazioni	Crea dashboard incentrati su metriche e osservazioni pertinenti per i tuoi sistemi e carichi di lavoro, per favorire 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. MoltiAWS servizi forniscono automaticamente le CloudWatch metriche, oltre all'integrazione dei CloudWatch registri 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 senza server. Questa guida include anche i seguentiAWS servizi utilizzati per la registrazione e il monitoraggio:

- AWS Systems ManagerDistributore, Systems Manager State Manager e Systems Manager Automation per automatizzare, configurare e aggiornare l' CloudWatch agente per le istanze EC2 e i server locali
- OpenSearch Servizio Amazon per l'aggregazione, la ricerca e l'analisi avanzate dei log
- Controlli di integrità 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 Amazon OpenSearch Service e Amazon Timestream) CloudWatch

I servizi diAWS elaborazione scelti influiscono anche sull'implementazione e sulla configurazione della soluzione di registrazione e monitoraggio. Ad esempio, CloudWatch l'implementazione e 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 dell'applicazione per i log e le metriche delle applicazioni. La guida fornisce un approccio consigliato per indirizzare questi due livelli attraverso diversi tipi di elaborazione, inclusi i tre tipi di elaborazione descritti nella tabella seguente.

Istanze EC2 immutabili e di lunga durata	Log e metriche di sistema e applicazioni su più sistemi operativi (OS) in piùAWS regioni o account.
Contenitori	Log e metriche di sistema e applicazioni per i cluster Amazon ECS e Amazon EKS, inclusi esempi di diverse configurazioni.
Serverless	Log e metriche di sistema e applicazioni per le funzioni Lambda e considerazioni per la personalizzazione.

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

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

- Configurazione della CloudWatch Agente per istanze EC2 e server locali— dettagli CloudWatch di configurazione per la registrazione e le metriche a livello di sistema e di applicazione.
- Approcci di installazione dell'agente CloudWatch per Amazon EC2 e server locali— Approcci per l'installazione dell' CloudWatch agente, inclusa la distribuzione automatizzata tramite Systems Manager in più regioni e account.
- Registrazione e monitoraggio su Amazon ECS — Linee guida CloudWatch per la configurazione dei log e delle metriche a livello di cluster e di applicazione in Amazon ECS.
- Registrazione e monitoraggio su Amazon EKS — Linee guida CloudWatch per la configurazione della registrazione e delle metriche a livello di cluster e di applicazione in Amazon EKS.
- Monitoraggio Prometheus su Amazon EKS— Introduce e confronta Amazon Managed Service per Prometheus con il monitoraggio di CloudWatch Container Insights per Prometheus.
- Registrazione e metriche perAWS 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 estendendo l'analisi dei log ad Amazon OpenSearch Service.
- Opzioni allarmanti con CloudWatch— Introduce gli CloudWatch allarmi e il rilevamento delle 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.
- Applicazioni di tracciamento conAWS X-Ray— Introduzione e configurazione per il tracciamento delle applicazioni tramite 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 iAWS carichi di lavoro.
- Integrazione con CloudWatch conAWSservizi— Spiega come CloudWatch si integra con variAWS servizi.
- Amazon Managed Grafana per dashboard e visualizzazione— Introduce e confronta Amazon Managed Grafana con CloudWatch per la dashboard e la visualizzazione.

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

Obiessi aziendali mirati

Creazione di una soluzione di registrazione e monitoraggio progettata perAWSIl cloud è parte integrante per il raggiungimento delsei 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. Puoi aspettarti i seguenti quattro risultati dopo aver implementato una soluzione di registrazione e monitoraggio allineata conAWSFramework Well-Architected:

Accelera la prontezza operativa

L'abilitazione di una soluzione di registrazione e monitoraggio è un componente importante per la preparazione di un carico di lavoro per il supporto e l'uso della produzione. La prontezza operativa può diventare rapidamente un collo di bottiglia se si fa troppo affidamento su processi manuali e può anche ridurre il time to value (TTV) per gli investimenti IT. Un approccio inefficace comporta anche un'osservabilità limitata dei carichi di lavoro. Ciò può aumentare il rischio di interruzioni prolungate, insoddisfazione del cliente e processi aziendali falliti.

È possibile utilizzare gli approcci di questa guida per standardizzare e automatizzare la registrazione e il monitoraggio sulAWSCloud. I nuovi carichi di lavoro richiedono quindi una preparazione manuale e un intervento minimi per la registrazione e il monitoraggio della produzione. Ciò consente inoltre di 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 molteplici best practice per la registrazione e il monitoraggio che aiutano diversi carichi di lavoro a soddisfare gli obiettivi aziendali eeccellenza operativa. Questa guida fornisce ancheesempi dettagliati e modelli open-source e riutilizzabiliche è possibile utilizzare con un approccio IAC (Infrastructure as code) per implementare una soluzione di registrazione e monitoraggio ben architettata utilizzandoAWSServizi . Migliorare l'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 risorse IT diverse e ospitate su diversi tipi di elaborazione, sia in locale che suAWSCloud. 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 nei carichi di lavoro. Questa guida ti aiuta a progettare e implementare approcci per migliorare la visibilità operativa completa e ridurre i guasti del tempo medio di risoluzione (MTTR). Un approccio completo di registrazione e monitoraggio aiuta anche l'organizzazione a migliorare la qualità del servizio, migliorare l'esperienza dell'utente finale e rispettare gli SLA (Service Level Agreement).

Ridimensiona le operazioni e riduci i costi generali

È possibile scalare le pratiche di registrazione e monitoraggio di questa guida per supportare più regioni e account, risorse di breve durata e più ambienti. La guida fornisce approcci ed esempi per automatizzare i passaggi manuali (ad esempio l'installazione e la configurazione degli agenti, il monitoraggio delle metriche e la notifica o l'azione in caso di problemi). Questi approcci sono utili quando l'adozione del cloud matura e cresce e devi scalare le capacità operative 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 dei carichi di lavoro e delle architetture esistenti.
- I tipi di elaborazione e i sistemi operativi che devono essere registrati e monitorati.
- Se sono presenti 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 più sistemi operativi e 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 sistemi operativi e ambienti. 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

- Gestione dei file di configurazione degli agenti CloudWatch

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.

	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 fino al livello di campo per i tuoi log. 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 proprieta ri 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'arch itettura 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 è possibile 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 effettuare il provisioning 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 log e metriche dai tuoi account e inviare dati a un account centralizzato o altra destinazione per ulteriori elaborazioni e monitoraggio.

Gestione dei file di configurazione degli agenti 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 tue 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' CloudWatchagente 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.

/config/standard/windows/ec2	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 configurazione standard specifici di Windows per i server locali. CloudWatch In questa cartella puoi inoltre classificare ulteriormente le configurazioni del sistema operativo standard per diverse versioni di Windows, tipi di server e ambienti.
/config/standard/linux/ec2	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 per i server locali. CloudWatch 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 monitoraggio a livello di sistema specifici di Amazon ECS.
/config/ <application_name>	Archivia i file di configurazione specifici dell'applicazione CloudWatch . È possibile classificare 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, GitHub o AWS CodeCommit) per archiviare i file di configurazione. 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 account e regioni.

Configurazione della CloudWatch Agente per istanze EC2 e server locali

Molte organizzazioni eseguono carichi di lavoro sia su server fisici che su macchine virtuali (VM). Questi carichi di lavoro in genere vengono eseguiti su sistemi operativi diversi che hanno requisiti di installazione e configurazione specifici per l'acquisizione e l'acquisizione di metriche.

Se si sceglie di utilizzare le istanze EC2, è possibile avere un alto livello di controllo sulla configurazione dell'istanza e del sistema operativo. Tuttavia, questo livello superiore di controllo e responsabilità richiede di monitorare e regolare le 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 standard di installazione e configurazione per l'acquisizione e l'acquisizione di log e metriche.

Organizations che migrano o estendono i loro investimenti IT alAWSIl cloud può sfruttare CloudWatch per ottenere una soluzione unificata di registrazione e monitoraggio. CloudWatch il pricing significa che paghi in modo incrementale le metriche e i log che desideri acquisire. È inoltre possibile acquisire registri e metriche per i server locali utilizzando uno strumento simile CloudWatch processo di installazione dell'agente come quello per Amazon EC2.

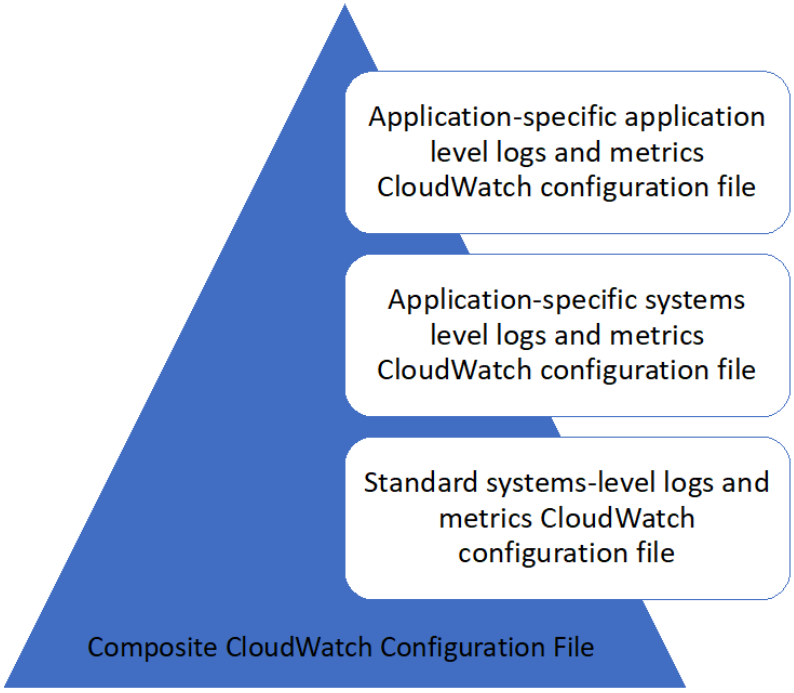
Prima di iniziare l'installazione e la distribuzione di CloudWatch, assicurati di valutare le configurazioni di registrazione e metrica per i sistemi e le applicazioni. Assicurati di definire i log e le metriche standard che devi acquisire per il sistema operativo che desideri utilizzare. I registri 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. Sono disponibili metriche e file di registro importanti nelle distribuzioni Linux, oltre a quelli specifici di una versione o distribuzione Linux. Questa varianza si verifica anche tra diverse versioni di Windows.

Configurazione della CloudWatch agente

CloudWatch acquisisce parametri e log per Amazon EC2 e da server locali utilizzandoAgenti CloudWatch e file di configurazione dell'agenteche sono specifici per ogni sistema operativo. Si consiglia di definire la configurazione standard della metrica e dell'acquisizione dei log dell'organizzazione prima di iniziare l'installazione CloudWatch agente su larga scala nei tuoi account.

Puoi combinare più CloudWatch configurazioni agente per formare un composito CloudWatch configurazione dell'agente. Un approccio consigliato è quello di definire e dividere le configurazioni

per i log e le metriche a livello di sistema e applicazione. Il seguente diagramma illustra come è possibile combinare più tipi di file di configurazione di CloudWatch per requisiti diversi per formare una configurazione composita di 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 i file di registro. Invece, i file di log vengono catturati e acquisiti in CloudWatch Registri del CloudWatch software Agente installato sull'istanza EC2,AWSAPI oAWS Command Line Interface(AWS CLI). Si consiglia di utilizzare CloudWatch agente in cui acquisire i file di log CloudWatch Registri per Amazon EC2 e server locali.

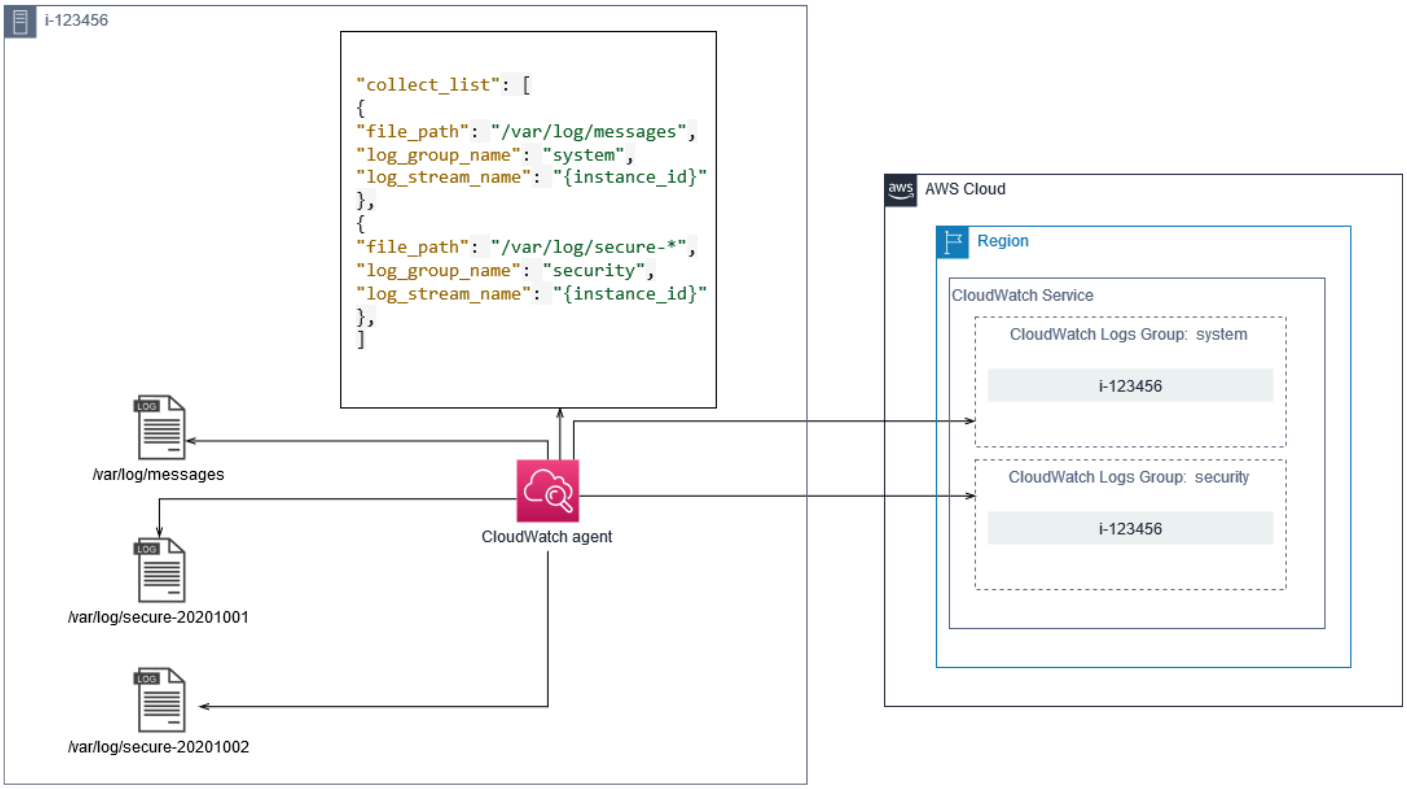
È possibile cercare e filtrare i log, estrarre le metriche ed eseguire l'automazione basata sull'applicazione di patch dei pattern dai file di log in CloudWatch. CloudWatch supporta opzioni di sintassi di filtro e pattern formattati in formato JSON, con log formattati in formato JSON che offrono

la massima flessibilità. Per aumentare le opzioni di filtraggio e analisi, è necessario utilizzare un output di log formattato anziché testo normale.

La CloudWatch agent utilizza un file di configurazione che definisce i log e le metriche da inviare a CloudWatch. CloudWatch quindi acquisisce ogni file di registro come aflusso di loge raggruppa questi flussi di log in agruppo di registri. Ciò consente di eseguire operazioni tra i log delle istanze EC2, ad esempio la ricerca di una stringa corrispondente.

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

Il seguente diagramma mostra un CloudWatch configurazione dell'agente per l'acquisizione dei registri. Il gruppo di log è definito dai file di log acquisiti e contiene flussi di log separati per ogni istanza EC2 perché`{instance_id}`la variabile viene utilizzata per il nome del flusso di log e gli ID di istanza EC2 sono univoci.



I gruppi di log definiscono la conservazione, i tag, la protezione, i filtri delle metriche e l'ambito di ricerca per i flussi di log in essi contenuti. Il comportamento di raggruppamento predefinito basato sul nome del file di registro aiuta a cercare, creare metriche e avvisi sui dati specifici di un file di log tra istanze EC2 in un account e in 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 business unit e avere proprietari tecnici o operativi diversi. Ciò significa che è necessario perfezionare 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, è possibile separare la registrazione per i carichi di lavoro eseguiti in ciascun ambiente. Nella tabella seguente viene illustrata una convenzione di denominazione del gruppo di log che include la business unit, 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 log	`<EC2 instance ID>`

È inoltre possibile raggruppare tutti i file di log per 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 servono un'applicazione o un carico di lavoro e ogni istanza EC2 ha uno scopo specifico. Nella tabella seguente viene illustrato come è possibile formattare il nome del gruppo di log e del flusso di log per supportare questo approccio.

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

Configurazione dell'acquisizione delle metriche per le istanze EC2

Per impostazione predefinita, le istanze EC2 sono abilitate per il monitoraggio base e aset standard di metriche(ad esempio, le metriche relative alla CPU, alla rete o allo storage) vengono automaticamente inviate a CloudWatch ogni cinque minuti. CloudWatch I parametri possono variare a seconda della famiglia di istanze, ad esempioistanze a prestazioni espandibilidispone di metriche per i crediti della CPU. Le metriche standard di Amazon EC2 sono incluse nel prezzo dell'istanza. Se abilitimonitoraggio dettagliatoPer le istanze EC2, puoi ricevere i dati in periodi di 1 minuto. La frequenza del periodo influisce sui costi di CloudWatch, quindi assicurati di valutare se è necessario un monitoraggio dettagliato per tutte o solo alcune istanze EC2. Ad esempio, è possibile abilitare il monitoraggio dettagliato dei carichi di lavoro di produzione ma utilizzare il monitoraggio di base per carichi di lavoro non di produzione.

I server locali non includono metriche predefinite per CloudWatch e deve utilizzare il plugin CloudWatch agente,AWS CLI, oppureAWSSDK per acquisire le metriche. Ciò significa che è necessario definire le metriche che si desidera acquisire (ad esempio, utilizzo della CPU) nel CloudWatch file di configurazione. Puoi creare un unico CloudWatch file di configurazione che include le metriche di istanza EC2 standard per i server locali e lo applica in aggiunta allo standard CloudWatch Configurazione di

Parametrinel CloudWatch sono definiti in modo univoco dal nome della metrica e da nessuna o più dimensioni e sono raggruppati in modo univoco in uno spazio dei nomi dei parametri. Metriche fornite da unAWSil servizio ha uno spazio dei nomi che inizia con`AWS`(ad esempio,`AWS/EC2`) e non-AWSI parametri sono considerati parametri personalizzati. Metriche che configuri e acquisisci con CloudWatch agent sono tutti considerati metriche personalizzate. Perché il numero di metriche create influisce sul tuo CloudWatch costi, è necessario valutare se ogni metrica è richiesta per tutte o solo alcune 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 queste metriche per carichi di lavoro non di produzione.

`CWAgent`è lo spazio dei nomi predefinito per le metriche pubblicate dal CloudWatch agente. Analogamente ai gruppi di log, lo spazio dei nomi delle metriche organizza una serie di metriche in modo che possano essere trovate insieme in un'unica posizione. È necessario modificare lo spazio dei nomi per riflettere una business unit, 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. Puoi anche correlare la

tua convenzione di denominazione dello spazio dei nomi con la tua CloudWatch convenzione di denominazione del gruppo di log.

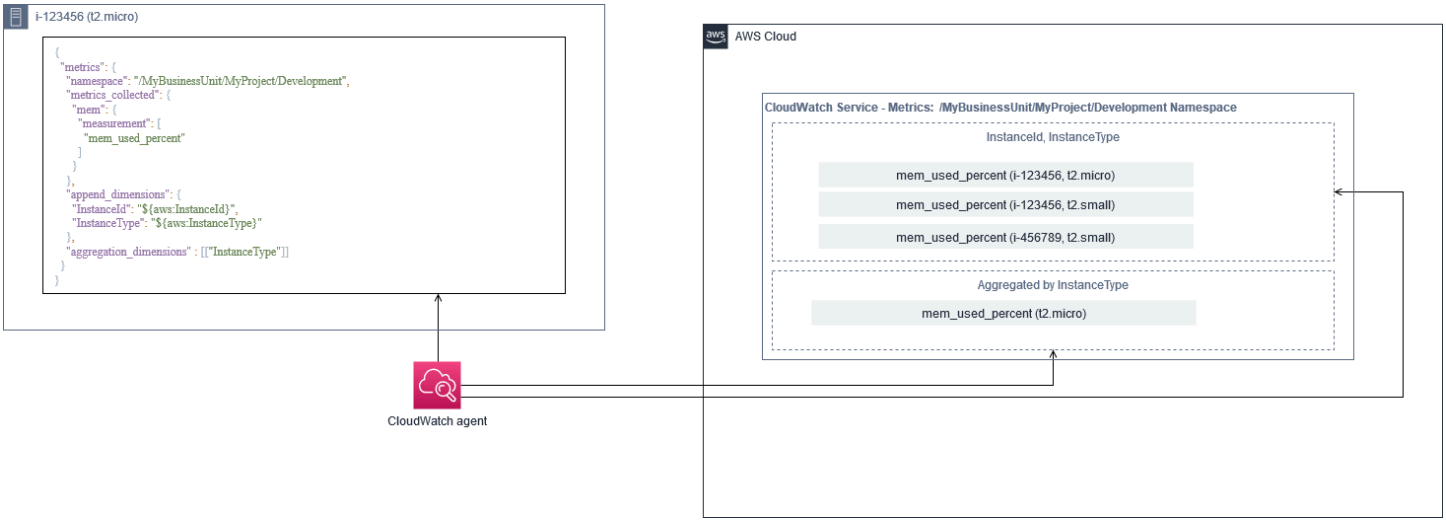
Le metriche sono identificate anche dalle loro dimensioni, che consentono di analizzarle in base a un insieme di condizioni e sono le proprietà sulle quali vengono registrate le osservazioni. Amazon EC2 includeparametri separatiper le istanze EC2 con`InstanceId`e`AutoScalingGroupName`dimensioni. Riceverai anche le metriche con`ImageId`e`InstanceType`dimensioni se si abilita il monitoraggio dettagliato. Ad esempio, Amazon EC2 fornisce una metrica di istanza EC2 separata per l'utilizzo della CPU con`InstanceId`dimensioni, oltre alla metrica di utilizzo della CPU separata per il`InstanceType`dimensione. Ciò consente di analizzare l'utilizzo della CPU per ogni istanza EC2 univoca, oltre a tutte le istanze EC2 di uno specificotipo di istanza.

L'aggiunta di più dimensioni aumenta la capacità di analisi, ma aumenta anche i costi complessivi, poiché ogni metrica e combinazione di valori di dimensione univoca si traduce in una nuova metrica. Ad esempio, se si crea una metrica per la percentuale di utilizzo della memoria rispetto al`InstanceId`dimension, quindi questa è una nuova metrica per ogni istanza EC2. Se l'organizzazione esegue migliaia di istanze EC2, ciò causa migliaia di metriche e si traduce in costi più elevati. Per controllare e prevedere i costi, assicurati di determinare la cardinalità della metrica e quali dimensioni aggiungono più valore. Ad esempio, è possibile definire un set completo di dimensioni per le metriche del carico di lavoro di produzione, ma un sottoinsieme più piccolo di queste dimensioni per carichi di lavoro non di produzione.

Puoi utilizzare il plugin`append_dimensions`proprietà per aggiungere dimensioni a una o tutte le metriche definite nel tuo CloudWatch Configurazione di È inoltre possibile aggiungere dinamicamente il`ImageId`,`InstanceId`,`InstanceType`, e`AutoScalingGroupName`a tutte le metriche nella tua CloudWatch Configurazione di In alternativa, è possibile aggiungere un nome e un valore di dimensione arbitrari per metriche specifiche utilizzando il`append_dimensions`proprietà su quella metrica. CloudWatch può anche aggregare statistiche sulle dimensioni metriche definite con il`aggregation_dimensions`proprietà.

Ad esempio, puoi aggregare la memoria utilizzata rispetto al`InstanceType`dimensione per vedere la memoria media utilizzata da tutte le istanze EC2 per ogni tipo di istanza. Se utilizzi`t2.micro`istanze in esecuzione in una regione, è possibile determinare se i carichi di lavoro utilizzano il`t2.micro`class sta sfruttando eccessivamente o sottoutilizzo della 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 seguente diagramma mostra un esempio CloudWatch configurazione delle metriche che utilizza uno spazio dei nomi personalizzato, dimensioni aggiunte e aggregazione per`InstanceType`.



A livello di sistema CloudWatch configurazione

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

Ti consigliamo di utilizzare il pluginProcedura guidata CloudWatch il file di configurazione dio schema del file di configurazione per definire il CloudWatch file di configurazione dell'agente per ogni sistema operativo che si intende supportare. I log e le metriche a livello di sistema operativo aggiuntivi specifici per il carico di lavoro possono essere definiti separatamente CloudWatch file di configurazione e aggiunti alla configurazione standard. Questi file di configurazione univoci devono essere memorizzati separatamente in un bucket S3 dove possono essere recuperati dalle istanze EC2. Un esempio di configurazione del bucket S3 per questo scopo è descritto nella sezioneGestione delle configurazioni CloudWatchsezione di questa guida. È possibile recuperare e applicare automaticamente queste configurazioni utilizzando State Manager e Distributor.

Configurazione dei log a livello di sistema

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

La CloudWatch agent supporta il monitoraggio dei registri eventi di Windows fornendo il nome del registro eventi. È possibile scegliere quali registri eventi di Windows si desidera monitorare (ad esempio`System`,`Application`, oppure`Security`).

I registri di sistema, applicazione e sicurezza per i sistemi Linux sono in genere memorizzati nel`/var/log`directory. La tabella seguente definisce i file di registro predefiniti comuni da monitorare, ma è necessario controllare il`/etc/rsyslog.conf`o`/etc/syslog.conf`file 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 dei kernel
	`/var/log/secure` — Registro di sicurezza e autenticazione
	`/var/log/messages` — Registro di sistema generale
	`/var/log/cron*` — Cron log
	`/var/log/cloud-init-output.log` — Output di`Userdata`script di avvio
Debian	`/var/log/syslog` — Registro di avvio
(Ubuntu)	`/var/log/cloud-init-output.log` — Output di`Userdata`script di avvio
	`/var/log/auth.log` — Registro di sicurezza e autenticazione
	`/var/log/kern.log` — Registro dei kernel

L'organizzazione potrebbe avere anche altri agenti o componenti di sistema che generano i log che si desidera monitorare. È necessario valutare e decidere quali file di registro vengono generati da questi agenti o applicazioni e includerli nella configurazione identificandone la posizione. Ad esempio, è

necessario includere Systems Manager e CloudWatch l'agente accede alla configurazione. La tabella seguente fornisce la posizione di questi log degli agenti per Windows e Linux.

Windows	Agente di CloudWatch	`$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log`

	Agente di Systems Manager	`%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log`
		`%PROGRAMDATA%\Amazon\SSM\Logs\errors.log`
		`%PROGRAMDATA%\Amazon\SSM\Logs\audits\amazon-ssm-agent-audit-YYYY-MM-DD`

Linux	Agente di CloudWatch	`/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log`

	Agente di Systems Manager	`/var/log/amazon/ssm/amazon-ssm-agent.log`
		`/var/log/amazon/ssm/errors.log`
		`/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 CloudWatch configurazione dell'agente ma non trovata. Ciò è utile quando si desidera mantenere una singola configurazione di log per Linux, anziché configurazioni separate per ogni distribuzione. È utile anche quando un file di registro non esiste fino all'avvio dell'esecuzione dell'agente o dell'applicazione software.

Configurazione dei parametri a livello di sistema

L'utilizzo di memoria e spazio su disco non è incluso nelle metriche standard fornite da Amazon EC2. Per includere queste parametri, è necessario installare e configurare CloudWatch agente sulle istanze EC2. La CloudWatch La procedura guidata di configurazione dell'agente crea un CloudWatch configurazione conparametri predefinitie puoi aggiungere o rimuovere parametri se necessario. Assicurati di rivedere i set di metriche predefiniti per determinare il livello appropriato richiesto.

Gli utenti finali e i proprietari del carico di lavoro devono pubblicare ulteriori metriche di sistema in base a requisiti specifici per un server o un'istanza EC2. Queste definizioni delle metriche devono essere memorizzate, controllate e mantenute in modo separato CloudWatch file di configurazione dell'agente e condiviso in una posizione centrale (ad esempio Amazon S3) per il riutilizzo e l'automazione.

Le metriche Amazon EC2 standard non vengono acquisite automaticamente nei server locali. Tali parametri devono essere definiti in a CloudWatch file di configurazione 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.

A livello di applicazione CloudWatch configurazione

I log e le metriche delle applicazioni vengono generati dall'esecuzione delle applicazioni e sono specifici per l'applicazione. Assicurati di definire i log e le metriche necessari per monitorare adeguatamente le applicazioni che vengono regolarmente utilizzate dall'organizzazione. Ad esempio, l'organizzazione potrebbe essere stata standardizzata su Microsoft Internet Information Server (IIS) per applicazioni basate sul Web. È possibile creare un registro e una metrica standard CloudWatch configurazione 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 del carico di lavoro o tramite il recupero automatico e copiati nella CloudWatch directory di configurazione. La CloudWatch agent combina automaticamente i file di configurazione di CloudWatch trovati nella directory dei file di

configurazione di ogni istanza o server EC2 in un composito CloudWatch Configurazione di Il risultato finale è un CloudWatch configurazione che include la configurazione standard a livello di sistema dell'organizzazione e tutti i livelli di applicazione pertinenti CloudWatch configurazioni.

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 commerciale off-the-shelf (COTS) o applicazione personalizzata. Le applicazioni COTS e i relativi componenti potrebbero fornire diverse opzioni per la configurazione e l'output del registro, come il livello di dettaglio del registro, il formato del file di registro e la posizione del file di registro. Tuttavia, la maggior parte delle applicazioni COTS o di terze parti non consentono di modificare fondamentalmente la registrazione (ad esempio, l'aggiornamento del codice dell'applicazione per includere istruzioni di log o formati aggiuntivi non configurabili). Come minimo, è necessario configurare le opzioni di registrazione per COTS o applicazioni di terze parti per registrare informazioni di avviso e di errore, preferibilmente in formato JSON.

È possibile integrare applicazioni sviluppate su misura con CloudWatch Registra includendo i file di registro dell'applicazione nel tuo CloudWatch Configurazione di Le applicazioni personalizzate offrono una migliore qualità e controllo dei log in quanto è possibile personalizzare il formato di output del registro, classificare e separare l'output dei componenti in modo da separare i file di registro, oltre a includere ulteriori dettagli richiesti. Assicurati di rivedere e standardizzare le librerie di registrazione e i dati e la formattazione necessari per la tua organizzazione in modo che l'analisi e l'elaborazione diventino più facili.

Puoi anche scrivere a CloudWatch flusso di log con CloudWatch Log`PutLogEvents`Chiamata API o utilizzando ilAWSSDK. È possibile utilizzare l'API o l'SDK per requisiti di registrazione personalizzati, come il coordinamento della registrazione a un singolo flusso di log su un set distribuito di componenti e server. Tuttavia, la soluzione più semplice da mantenere e più applicabile è configurare le applicazioni in modo da scrivere su file di registro e quindi utilizzare il CloudWatch agente per leggere e trasmettere i file di registro su 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, creare grafici e allarmi su questi dati in un CloudWatch gruppo di log. Ad esempio, è possibile utilizzare un filtro metrico per contare i tentativi di accesso non riusciti identificandoli nei registri.

Puoi anche creare metriche personalizzate per le tue applicazioni sviluppate su misura utilizzando ilParametri integrati CloudWatchformatonei file di registro dell'applicazione.

Configurazione dei parametri a livello di applicazione

Le metriche personalizzate sono metriche che non vengono fornite direttamente daAWSservizi a CloudWatch e sono pubblicati in uno spazio dei nomi personalizzato in CloudWatch Parametri di Tutte le metriche delle applicazioni sono considerate personalizzate CloudWatch Parametri di Le metriche delle applicazioni potrebbero essere allineate a un'istanza EC2, un componente dell'applicazione, una chiamata API o persino a una funzione aziendale. È inoltre necessario considerare l'importanza e la cardinalità delle dimensioni che scegli per le tue metriche. Le dimensioni con elevata cardinalità generano un gran numero di metriche personalizzate e potrebbero aumentare la tua CloudWatch costi.

CloudWatch ti aiuta a catturare le metriche a livello di applicazione in diversi modi, tra cui:

- Acquisizione delle metriche a livello di processo definendo i singoli processi che si desidera acquisire dalplugin procstat.
- Un'applicazione pubblica una metrica in Windows Performance Monitor e questa metrica è definita nella CloudWatch Configurazione di
- I filtri e i pattern metrici vengono applicati ai registri di un'applicazione in CloudWatch.
- Un'applicazione scrive su un CloudWatch registri utilizzando il plugin CloudWatch formato dei parametri incorporato.
- Un'applicazione invia una metrica a CloudWatch tramite API oAWSSDK.
- Un'applicazione invia una metrica araccoltooStatsDdemone con configurato CloudWatch agente.

È possibile utilizzare procstat per monitorare e misurare i processi applicativi critici con l'agente CloudWatch. Ciò consente di lanciare un allarme e di intervenire (ad esempio, un processo di notifica o 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 lanciare un allarme se un determinato processo agisce in modo anomalo.

Il monitoraggio di Procstat è utile anche se non è possibile aggiornare le applicazioni COTS con metriche personalizzate aggiuntive. Ad esempio, è possibile creare un`my_process`metrica che misura il`cpu_time`e include una personalizzazione`application_version`dimensione. È possibile utilizzare anche più CloudWatch file di configurazione agente per un'applicazione se si dispone di 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, 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.

Assicurati di rivedere 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 rivedere i registri cronologici per l'applicazione per determinare come vengono rappresentati i messaggi di errore e gli spegnimenti anomali. È inoltre necessario esaminare i problemi segnalati in precedenza per determinare se è possibile acquisire una metrica per evitare che il problema si ripeta. È inoltre necessario rivedere la documentazione dell'applicazione e chiedere agli sviluppatori dell'applicazione di confermare il modo in cui i messaggi di errore possono essere identificati.

Per le applicazioni sviluppate su misura, collabora con gli sviluppatori dell'applicazione per definire metriche importanti che possono essere implementate utilizzando il CloudWatch formato dei parametri incorporato,AWSSDK oAWSAPI. L'approccio consigliato consiste nell'utilizzare il formato metrico incorporato. Puoi utilizzare il pluginAWSha fornito librerie di formati metrici incorporati open-source per aiutarti a scrivere le tue istruzioni nel formato richiesto. Dovresti anche aggiornare il tuospecifica dell'applicazione CloudWatch configurazioneper includere l'agente di formato dei parametri incorporato. Ciò fa sì che l'agente in esecuzione sull'istanza EC2 funga da endpoint del formato metrico incorporato locale che invia metriche incorporate al formato metrico a CloudWatch.

Se le tue applicazioni supportano già la pubblicazione di metriche da raccogliere o dichiarare, puoi sfruttarle per acquisire metriche in CloudWatch.

Approcci di installazione dell'agente CloudWatch per Amazon EC2 e server locali

Automazione di CloudWatch Il processo di installazione dell'agente ti aiuta a distribuirlo in modo rapido e coerente e a catturare i log e le metriche richiesti. Esistono diversi approcci per automatizzare l'installazione dell'agente CloudWatch, incluso il supporto multi-account e multi-regione. Vengono discussi i seguenti approcci di installazione automatizzata:

- Installazione di CloudWatch agente che utilizza Systems Manager Distributor e Systems Manager State Manager— Si consiglia di utilizzare questo approccio se le istanze EC2 e i server locali utilizzano l'agente Systems Manager. Ciò garantisce che il CloudWatch l'agente viene mantenuto aggiornato ed è possibile segnalare e correggere i server che non hanno CloudWatch Agente. Questo approccio è inoltre scalabile per supportare più account e regioni.
- Distribuzione di CloudWatch agente come parte dello script di dati utente durante il provisioning dell'istanza EC2— Amazon EC2 consente di definire uno script di avvio che viene eseguito al primo avvio o al riavvio. È possibile definire uno script per automatizzare il processo di download e installazione dell'agente. Questo può essere incluso anche inAWS CloudFormationscript eAWSProdotti Service Catalog. Questo approccio potrebbe essere appropriato in base alle necessità se esiste un approccio personalizzato per l'installazione e la configurazione dell'agente per un carico di lavoro specifico che si discosta dagli standard.
- Incluso l'agente CloudWatch in Amazon Machine Image (AMI)— È possibile installare l'agente CloudWatch nelle AMI personalizzate per Amazon EC2. Le istanze EC2 che utilizzano l'AMI avranno automaticamente installato e avviato l'agente. Tuttavia, è necessario assicurarsi che l'agente e la sua configurazione siano regolarmente aggiornati.

Installazione di CloudWatch agente che utilizza Systems Manager Distributor e State Manager

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

Questo approccio all'installazione ha i seguenti requisiti preliminari:

- 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 alcune AMI. L'agente deve anche essere installato e configurato su altre immagini o VM e server locali.
- Un ruolo IAM o credenziali che hannonecessario CloudWatch e autorizzazioni Systems Managerdeve essere collegato all'istanza EC2 o definito nel file delle credenziali per un server locale. Ad esempio, è possibile creare un ruolo IAM che includeAWSpolicy gestite:`AmazonSSMManagedInstanceCore`per Systems Manager e`CloudWatchAgentServerPolicy`per CloudWatch. Puoi utilizzare il pluginssm-cloudwatch-instance-role.yaml AWS CloudFormationModello per distribuire un ruolo e un profilo di istanza IAM che include entrambi i criteri. Questo modello può anche essere modificato per includere altre autorizzazioni IAM standard per le istanze EC2. Per server o macchine virtuali o server locali, è necessario configurare CloudWatch per utilizzareRuolo del servizio Systems Managerconfigurato per il server locale. Per ulteriori informazioni, consultaCome posso configurare i server locali che utilizzano Systems Manager Agent e l'unificato CloudWatch agente per utilizzare solo credenziali temporanee?nellaAWSKnowledge Center.

L'elenco seguente offre diversi vantaggi per l'utilizzo dell'approccio Systems Manager Distributor e State Manager per installare e mantenere il CloudWatch agente:

- Installazione automatica per più sistemi operativi— Non è necessario scrivere e mantenere uno script per ciascun sistema operativo per scaricare e installare l'agente CloudWatch.
- Controlli dell'aggiornamento automatico— State Manager verifica automaticamente e regolarmente che ogni istanza EC2 abbia la versione più recente di CloudWatch.
- Report sulla conformità— Il dashboard di conformità di Systems Manager mostra quali istanze EC2 non sono riuscite a installare correttamente il pacchetto Distributor.
- Installazione automatizzata per istanze EC2 appena lanciate— Le nuove istanze EC2 che vengono lanciate nel tuo account ricevono automaticamente il CloudWatch Agente.

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

- Collisione con un'associazione esistente— Se un'altra associazione già installa o configura il CloudWatch agente, quindi 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'agente e la configurazione di CloudWatch.

- Aggiornamento di file di configurazione dell'agente personalizzato— Distributor esegue un'installazione utilizzando il file di configurazione predefinito. Se si utilizza un file di configurazione personalizzato o multiplo CloudWatch file di configurazione, è necessario aggiornare la configurazione dopo l'installazione.
- Configurazione multi-regione o multi-account— L'associazione di State Manager deve essere istituita in ogni account e regione. I nuovi account in un ambiente multi-account devono essere aggiornati per includere l'associazione State Manager. È necessario centralizzare o sincronizzare il CloudWatch configurazione in modo che più account e regioni possano recuperare e applicare gli standard richiesti.

Impostare State Manager e Distributore per CloudWatch distribuzione e configurazione dell'agente

È possibile utilizzareConfigurazione rapida Systems Managerper configurare rapidamente le funzionalità di Systems Manager, inclusa l'installazione e l'aggiornamento automatico del CloudWatch agente sulle istanze EC2. Quick Setup distribuisce unAWS CloudFormationstack che distribuisce e configura le risorse di Systems Manager in base alle tue scelte.

L'elenco seguente fornisce due importanti azioni eseguite da Quick Setup per l'automazione CloudWatch installazione e aggiornamento dell'agente:

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 potrebbero variare ma il contenuto rimane invariato:
   - `CreateAndAttachIAMToInstance`— Crea il`AmazonSSMRoleForInstancesQuickSetup`ruolo e profilo di istanza se non esistono e allegano il`AmazonSSMManagedInstanceCore`policy per il ruolo. Questo non include il richiesto`CloudWatchAgentServerPolicy`Policy IAM. È necessario aggiornare questo criterio e aggiornare il documento di Systems Manager per includere questo criterio come descritto nella sezione seguente.
   - `InstallAndManageCloudWatchDocument`— Installa il file CloudWatch agente con Distributor e configura ogni istanza EC2 una volta con un valore predefinito CloudWatch configurazione dell'agente utilizzando il`AWS-ConfigureAWSPackage`Documento di Systems Manager.

- `UpdateCloudWatchDocument`— Aggiornamento di CloudWatch agente installando l'agente CloudWatch più recente tramite`AWS-ConfigureAWSPackage`Documento di Systems Manager. L'aggiornamento o la disinstallazione dell'agente non rimuove l'esistente CloudWatch file di configurazione dall'istanza EC2.

2. Creazione di associazioni State Manager— Le associazioni di State Manager vengono create e configurate per utilizzare i documenti di Systems Manager creati personalizzati. I nomi delle associazioni di State Manager potrebbero variare ma la configurazione rimane la stessa:
   - `ManageCloudWatchAgent`— Esegue`InstallAndManageCloudWatchDocument`Documento di Systems Manager una volta per ogni istanza EC2.
   - `UpdateCloudWatchAgent`— Esegue`UpdateCloudWatchDocument`Documento di Systems Manager ogni 30 giorni per ogni istanza EC2.
   - Eseguire`CreateAndAttachIAMToInstance`Documento di Systems Manager una volta per ogni istanza EC2.

È necessario aumentare e personalizzare la configurazione Quick Setup completata per includere le autorizzazioni di CloudWatch e il supporto personalizzato CloudWatch configurazioni. In particolare,`CreateAndAttachIAMToInstance`e la`InstallAndManageCloudWatchDocumen`til documento dovrà essere aggiornato. È possibile aggiornare manualmente i documenti di Systems Manager creati da Quick Setup. In alternativa, è possibile utilizzare il proprio CloudFormation modello per il provisioning delle stesse risorse con gli aggiornamenti necessari, nonché configurare e distribuire altre risorse di Systems Manager e non utilizzare Quick Setup.

> **Important**
>
> Configurazione rapida crea unAWS CloudFormationstack 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 aggiornare manualmente i documenti di Systems Manager.

Nelle sezioni seguenti viene descritto come aggiornare manualmente le risorse di Systems Manager create da Quick Setup, nonché utilizzare le proprieAWS CloudFormationmodello per eseguire una configurazione rapida aggiornata. Ti consigliamo di utilizzare il proprioAWS CloudFormationmodello per evitare l'aggiornamento manuale delle risorse create da Quick Setup eAWS CloudFormation.

Utilizzare Systems Manager Quick Setup e aggiornare manualmente le risorse di Systems Manager create

Le risorse di Systems Manager create con l'approccio Quick Setup devono essere aggiornate in modo da includere il necessario CloudWatch autorizzazioni agente e supporto multiplo CloudWatch file di configurazione. Questa sezione descrive come aggiornare il ruolo IAM e i documenti di Systems Manager per utilizzare un bucket S3 centralizzato contenente CloudWatch configurazioni accessibili da più account. Creazione di un bucket S3 per archiviare CloudWatch i file di configurazione sono discussi nelGestione delle configurazioni CloudWatchsezione di questa guida.

Aggiornamento di**`CreateAndAttachIAMToInstance`**Documento di Systems Manager

Questo documento di Systems Manager creato da Quick Setup verifica se a un'istanza EC2 è associato un profilo di istanza IAM esistente. Se lo fa, si attacca il`AmazonSSMManagedInstanceCore`politica per il ruolo esistente. Questo protegge le istanze EC2 esistenti dalla perditaAWSautorizzazioni che potrebbero essere assegnate tramite profili di istanza esistenti. È necessario aggiungere un passaggio in questo documento per allegare`CloudWatchAgentServerPolicy`Criteri IAM alle istanze EC2 che hanno già un profilo di istanza collegato. Il documento Systems Manager crea anche il ruolo IAM se non esiste e un'istanza EC2 non ha un profilo di istanza allegato. È necessario aggiornare questa sezione del documento per includere anche il`CloudWatchAgentServerPolicy`Policy IAM.

Esaminare il file completatoCrea e allega chiam.YAMLdocumento di esempio e confrontarlo con il documento creato da Quick Setup. Modificare 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, quindi assicurati di apportare le modifiche necessarie. Il documento di esempio include l'opzione Configurazione rapida per eseguire la scansione giornaliera delle istanze alla ricerca di patch mancanti e pertanto include un criterio per Systems Manager Patch Manager.

Aggiornamento di**`InstallAndManageCloudWatchDocument`**Documento di Systems Manager

Questo documento di Systems Manager creato da Quick Setup installa il CloudWatch agente e lo configura con il valore predefinito CloudWatch configurazione dell'agente. Il valore di timeout predefinito per CloudWatch configurazione si allinea al set di metriche di base predefinito. È

necessario sostituire il passaggio di configurazione predefinito e aggiungere i passaggi per scaricare il CloudWatch file di configurazione dal tuo CloudWatch bucket di configurazione S3.

Esaminare il file completatoInstalla e gestisci il Cloud WatchDocument.YAMLdocumento aggiornato e confrontarlo con il documento creato da Quick Setup. Il documento creato da 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.

UtilizzaAWS CloudFormationanziché Configurazione rapida

Invece di utilizzare Configurazione rapida, è possibile utilizzareAWS CloudFormationper configurare Systems Manager. Questo approccio consente di personalizzare la configurazione di Systems Manager in base alle esigenze specifiche. Questo approccio evita inoltre aggiornamenti manuali delle risorse di Systems Manager configurate create da Quick Setup per supportare il supporto personalizzato. CloudWatch configurazioni.

La funzione Quick Setup utilizza ancheAWS CloudFormatione crea unAWS CloudFormationstack set per distribuire e configurare le risorse di Systems Manager in base alle tue scelte. Prima di poter utilizzareAWS CloudFormationset di stack, è necessario creare i ruoli IAM utilizzati daAWS CloudFormation StackSets per supportare le distribuzioni su più account o regioni. Quick Setup crea i ruoli necessari per supportare distribuzioni multi-regione o multi-account conAWS CloudFormationStackSets. È necessario completare i prerequisiti perAWS CloudFormation StackSets se si desidera configurare e distribuire le risorse di Systems Manager in più regioni o più account da un unico account e regione. Per ulteriori informazioni, consultaPrerequisiti per le operazioni dei set di stacknellaAWS CloudFormationdocumentazione.

Esaminare laAWS - Quicksetup-SSMHost MGMT.YAML AWS CloudFormationModello per Configurazione rapida personalizzata.

È necessario esaminare le risorse e le funzionalità delAWS CloudFormatione apportare modifiche in base alle tue esigenze. Dovresti controllare la versioneAWS CloudFormationmodello utilizzato e testare in modo incrementale le modifiche per confermare il risultato richiesto. Inoltre, è necessario eseguire revisioni sulla sicurezza cloud per determinare se sono necessarie modifiche alle policy in base ai requisiti dell'organizzazione.

È consigliabile distribuireAWS CloudFormationimpilare in un unico account di test e regione ed eseguire tutti i test case necessari per personalizzare e confermare il risultato desiderato. È quindi possibile graduare la distribuzione in più regioni in un unico account e quindi in più account e più regioni.

Configurazione rapida personalizzata in un singolo account e Regione conAWS CloudFormationpila

Se si utilizza solo un unico account e una regione, è possibile distribuire l'esempio completo comeAWS CloudFormationstack al posto di unAWS CloudFormationStack Set. Tuttavia, se possibile, ti consigliamo di utilizzare l'approccio con set di stack multi-account e multi-regione anche se usi solo un singolo account e una regione. Utilizzo diAWS CloudFormation StackSets facilita l'espansione a conti aggiuntivi e regioni in future.

Attenersi alla seguente procedura per distribuireAWS - Quicksetup-SSMHost MGMT.YAML AWS CloudFormationtemplate come unAWS CloudFormationstack in un singolo account e Regione:

1. Scarica il modello e verificalo nel tuo sistema di controllo della versione preferito (ad esempioAWS CodeCommit).
2. Personalizza il valore predefinitoAWS CloudFormationvalori dei parametri basati sui requisiti dell'organizzazione.
3. Personalizzare le pianificazioni dell'associazione di State Manager.
4. Personalizzare il documento Systems Manager con`InstallAndManageCloudWatchDocument`ID logico. Verificare che i prefissi del bucket S3 siano allineati ai prefissi per il bucket S3 contenente il CloudWatch Configurazione di
5. Recupera e registra il nome delle risorse Amazon (ARN) per il bucket S3 contenente CloudWatch configurazioni. Per ulteriori informazioni, consultaGestione delle configurazioni CloudWatchsezione di questa guida. Un esempiocloudwatch-config-s3-bucket.yaml AWS CloudFormationè disponibile un modello che include un criterio bucket per fornire l'accesso in letturaAWS Organizationsconti.
6. Distribuisci il Quick Setup personalizzatoAWS CloudFormationmodello sullo stesso account del tuo bucket S3:
   - Per il`CloudWatchConfigBucketARN`(Parametro), immetti l'ARN del bucket S3.
   - Effettuare le modifiche alle opzioni dei parametri in base alle funzionalità che si desidera abilitare per Systems Manager.

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

- Applicazione della`AttachIAMToInstance`Associazione 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 su base pianificata. Per ulteriori informazioni, consultaEsecuzione delle automazioni con attivazioni tramite State Managernella documentazione di Systems Manager.

- Verificare che all'istanza EC2 sia associato il ruolo IAM richiesto.
- Verificare che l'agente Systems Manager funzioni correttamente confermando che l'istanza EC2 è visibile in Systems Manager.
- Confermare che CloudWatch agente funziona correttamente visualizzando CloudWatch log e parametri basati sul CloudWatch configurazioni dal proprio bucket S3.

Configurazione rapida personalizzata in più regioni e account conAWS CloudFormationStackSets

Se si utilizzano più account e regioni, è possibile distribuireAWS - Quicksetup-SSMHost MGMT.YAML AWS CloudFormationmodello come set di stack. È necessario completare ilAWS CloudFormationPrerequisiti StackSetprima di utilizzare stack set. I requisiti variano a seconda che si stiano distribuendo set di stack congestito dal clienteogestito dal servizioautorizzazioni.

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 dalAWS Organizationsaccount di gestione o account amministratore delegato. È necessario distribuire lo stack set da un account centralizzato utilizzato per l'automazione con privilegi di amministratore delegati, anziché ilAWS Organizationsaccount di gestione. Si consiglia inoltre di testare la distribuzione del set di stack mirando a un'unità organizzativa di test (OU) con un numero singolo o piccolo di account in una regione.

1. Completa i passaggi da 1 a 5 dalConfigurazione rapida personalizzata in un singolo account e Regione conAWS CloudFormationpilasezione di questa guida.
2. Accedi allaAWS Management Console, aprireAWS CloudFormationconsoler e scegliCreazione di StackSet:
   - ScegliereTemplate is ready (Il modello è pronto)eUpload a template file (Carica un file modello). Carica il fileAWS CloudFormationmodello che hai personalizzato in base alle tue esigenze.
   - Specificare i dettagli del set di stack:
     - Immettere il nome di un set di stack, ad esempio`StackSet-SSM-QuickSetup`.

- Effettuare le modifiche alle opzioni dei parametri in base alle funzionalità che si desidera abilitare per Systems Manager.
- Per il`CloudWatchConfigBucketARN`parametro, immetti l'ARN per il tuo CloudWatch bucket S3 di configurazione.
- Specificare le opzioni del set di stack, scegliere se utilizzare le autorizzazioni gestite dai servizi conAWS Organizationso autorizzazioni gestite dall'utente.
  - Se scegli le autorizzazioni autogestite, inserisci ilRuolo di amministrazione del set di stack AWS Cloud FormationeRuolo di esecuzione del set di stack AWS Cloud FormationDettagli dei ruoli IAM. Il ruolo amministratore deve esistere nell'account e il ruolo di esecuzione deve esistere in ogni account di destinazione
- Pergestito dal servizioautorizzazioni conAWS Organizations, ti consigliamo innanzitutto di eseguire la distribuzione in un'unità organizzativa di test anziché sull'intera organizzazione.
  - Scegli se vuoi abilitare le distribuzioni automatiche. Ti consigliamo di scegliereEnabled (Abilitato). Per il comportamento di rimozione dell'account, l'impostazione consigliata èEliminazione degli stack.
- Pergestito dal clienteautorizzazioni, immettere ilAWSID account per gli account che vuoi impostare. È necessario ripetere questo processo per ogni nuovo account se si utilizzano autorizzazioni autogestite.
- Inserisci le regioni in cui utilizzerai CloudWatch e Systems Manager.
- Verificare che la distribuzione abbia esito positivo visualizzando lo stato nellaOperazioni eIstanze di stacktab per il set di stack.
- Testare il Systems Manager e CloudWatch funziona correttamente negli account distribuiti seguendo il passaggio 7 delConfigurazione rapida personalizzata in un singolo account e Regione conAWS CloudFormationpilasezione di questa guida.

Considerazioni per la configurazione di server locali

La CloudWatch agente per server locali e VM è installato e configurato utilizzando un approccio simile a quello per le istanze EC2. Tuttavia, la tabella seguente fornisce considerazioni che è necessario valutare durante l'installazione e la configurazione del CloudWatch agente su server e macchine virtuali.

Puntare CloudWatch agente alle stesse credenziali temporanee utilizzate per Systems Manager.	Quando si configura Systems Manager in un ambiente ibrido che include server locali, è possibile attivare Systems Manager con un ruolo IAM. È necessario utilizzare il ruolo creato per le istanze EC2 che include il`CloudWatch AgentServerPolicy` e `AmazonSSMManagedInstanceCore` politiche. Ciò comporta che l'agente Systems Manager recupera e scrive credenziali temporanee in un file di credenziali locali. Puoi puntare il tuo CloudWatch configurazione dell'agente nello stesso file. È possibile utilizzare il processo daConfigurare i server locali che utilizzano l'agente Systems Manager e l'agente CloudWatch unificato per utilizzare solo credenziali temporaneenellaAWSKnowledge Center. È inoltre possibile automatizzare questo processo definendo un runbook di Systems Manager Automation separato e un'associazione State Manager e indirizzando le istanze locali con i tag. Quando si crea un fileAttivazione di Systems Managerper le istanze locali, è necessario includere un tag che identifica le istanze come istanze locali.
Prendi in considerazione l'utilizzo di account e regioni con VPN oAWS Direct Connectaccesso eAWSPrivateLink.	È possibile utilizzareAWS Direct ConnectoAWS Virtual Private Network(AWS VPN) per stabilire connessioni private tra le reti locali e il cloud privato virtuale (VPC).AWS PrivateLink stabilisce una connessione privata a CloudWatch Log con un endpoint VPC dell'interfaccia. Questo approccio è utile se si dispone di restrizioni che

	impediscono l'invio di dati su Internet pubblico a un endpoint di servizio pubblico.
Tutte le metriche devono essere incluse nel CloudWatch File di configurazione.	Amazon EC2 include metriche standard (ad esempio l'utilizzo della CPU), ma queste metriche devono essere definite per le istanze locali. È possibile utilizzare un file di configura zione della piattaforma separato per definire queste metriche per i server locali e quindi aggiungere la configurazione allo standard. CloudWatch configurazione delle metriche per la piattaforma.

Considerazioni per istanze EC2 effimere

Le istanze EC2 sono temporanee oeffimero, se sono forniti da Amazon EC2 Auto Scaling, Amazon EMR,Istanze Spot Amazon EC2, oppureAWS Batch. Le istanze EC2 effimere possono causare un numero molto elevato di CloudWatch trasmette in streaming in un gruppo di log comune senza ulteriori informazioni sull'origine del runtime.

Se si utilizzano istanze EC2 effimere, prendere in considerazione l'aggiunta di ulteriori informazioni contestuali dinamiche nel gruppo di log e nei nomi dei flussi di log. Ad esempio, puoi includere l'ID richiesta dell'istanza Spot, il nome del cluster Amazon EMR o il nome del gruppo Auto Scaling. Queste informazioni possono variare per le istanze EC2 appena avviate e potrebbe essere necessario recuperarle e configurarle in fase di runtime. È possibile farlo scrivendo a CloudWatch file di configurazione dell'agente all'avvio e riavvio dell'agente per includere il file di configurazione aggiornato. Ciò consente la distribuzione di log e metriche a CloudWatch utilizzando informazioni di runtime dinamiche.

È inoltre necessario assicurarsi che le metriche e i registri siano inviati dal CloudWatch agente prima che le istanze EC2 effimere vengano terminate. La CloudWatch agente include un`flush_interval`parametro che può essere configurato per definire l'intervallo di tempo per il flushing log e i buffer metrici. È possibile ridurre questo valore in base al carico di lavoro e arrestare CloudWatch Agente e forza lo svuotamento dei buffer prima che l'istanza EC2 venga terminata.

Utilizzo di una soluzione automatizzata per implementare CloudWatch agente

Se si utilizza una soluzione di automazione (ad esempio, Ansible o Chef), è possibile utilizzarla per installare e aggiornare automaticamente il CloudWatch Agente. Se si utilizza questo approccio, è necessario valutare le seguenti considerazioni:

- Verifica che l'automazione copra i sistemi operativi e le versioni del sistema operativo supportate. Se lo script di automazione non supporta tutti i sistemi operativi dell'organizzazione, è necessario definire soluzioni alternative per i sistemi operativi non supportati.
- Verifica che la soluzione di automazione controlli regolarmente gli aggiornamenti e gli aggiornamenti dell'agente CloudWatch. La soluzione di automazione dovrebbe controllare regolarmente la presenza di aggiornamenti del CloudWatch agente o disinstalla e reinstalla regolarmente l'agente. È possibile utilizzare una funzionalità di pianificazione o di una soluzione di automazione per controllare e aggiornare regolarmente l'agente.
- Verifica che sia possibile confermare l'installazione dell'agente e la conformità alla configurazione. La soluzione di automazione dovrebbe consentire di determinare quando un sistema non ha installato l'agente o quando l'agente non funziona. È possibile implementare una notifica o un allarme nella soluzione di automazione in modo che le installazioni e le configurazioni non riuscite vengano monitorate.

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

È possibile utilizzare questo approccio se non si prevede di utilizzare Systems Manager e si desidera utilizzare in modo selettivo CloudWatch per le istanze EC2. In genere, questo approccio viene utilizzato una tantum o quando è richiesta una configurazione specializzata.AWSforniscelink direttiper CloudWatch agente che può essere scaricato negli script di dati di avvio o utente. I pacchetti di installazione dell'agente possono essere eseguiti in modo silenzioso senza interazione dell'utente, il che significa che è possibile utilizzarli nelle distribuzioni automatiche. Se si utilizza questo approccio, è necessario valutare le seguenti considerazioni:

- Rischio aumentato che gli utenti non installino l'agente o configurino metriche standard. Gli utenti possono eseguire il provisioning delle istanze senza includere i passaggi necessari per installare

il CloudWatch Agente. Potrebbero anche configurare in modo errato l'agente, il che potrebbe causare incongruenze di registrazione e monitoraggio.

- Gli script di installazione devono essere specifici per il 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 diversi passaggi di installazione in base alla distribuzione.
- È necessario aggiornare regolarmente il CloudWatch agente con nuove versioni quando disponibile. Questo può essere automatizzato se si utilizza Systems Manager con State Manager, ma è anche possibile configurare lo script dei dati utente da eseguire nuovamente all'avvio dell'istanza. La CloudWatch agente viene quindi aggiornato e reinstallato ad ogni riavvio.
- È necessario automatizzare il recupero e l'applicazione delle configurazioni CloudWatch standard. Questo può essere automatizzato 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 il file di configurazione CloudWatch Agente.

Includere il kit CloudWatch Agente nelle AMI

Il vantaggio di utilizzare questo approccio è che non è necessario attendere CloudWatch agente da installare e configurare ed è possibile iniziare immediatamente la registrazione e il monitoraggio. In questo modo è possibile monitorare meglio il provisioning delle istanze e i passaggi di avvio nel caso in cui le istanze non vengano avviate. 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:

- Deve esistere un processo di aggiornamento perché le AMI potrebbero non includere le più recenti CloudWatch Versione dell'agente. La CloudWatch l'agente installato in un'AMI è corrente solo all'ultima volta che è stata creata l'AMI. È necessario includere un metodo aggiuntivo per aggiornare regolarmente l'agente e quando viene eseguito il provisioning dell'istanza EC2. Se si utilizza Systems Manager, è possibile utilizzare il[Installazione di CloudWatch agente che utilizza Systems Manager Distributor e State Manager]soluzione fornita in questa guida per questo. Se non si utilizza Systems Manager, è possibile utilizzare uno script dati utente per aggiornare l'agente all'avvio e al riavvio dell'istanza.
- Il tuo CloudWatch il file di configurazione 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 il file di configurazione CloudWatch Agente.

- La CloudWatch agente deve essere riavviato dopo il tuo CloudWatch La configurazione è aggiornata.
- AWSle credenziali non devono essere salvate nell'AMI. Assicurarsi che non sia localeAWSle credenziali sono archiviate nell'AMI. Se utilizzi Amazon EC2, puoi applicare il ruolo IAM necessario alla tua istanza ed evitare credenziali locali. Se si utilizzano istanze locali, è necessario automatizzare o aggiornare manualmente le credenziali dell'istanza prima di avviare il CloudWatch Agente.

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 AWS Management Console per effettuare il provisioning di un cluster Amazon ECS con il tipo di avvio EC2, in modo da creare uno AWS 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 di CloudWatch agente che utilizza 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 AWS 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 le AMI e l'agente container ottimizzati più recenti per Amazon ECS. 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 le AMI

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

AWS fornisce gli stessi parametri Parameter Store in ogni regione supportata. Ciò significa che i AWS 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 nuove AMI Amazon ECS nella tua organizzazione facendo riferimento 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. AWS Management Console `/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 utilizzi una pipeline di integrazione e distribuzione continua (CI/CD) o un processo automatizzato, puoi creare una nuova revisione della definizione delle attività per la tua applicazione con ogni nuova build di immagine Docker. Ad esempio, puoi includere il nome dell'immagine Docker, il tag dell'immagine, la GitHub revisione o altre informazioni importanti nella revisione della definizione delle attività e nella configurazione della registrazione come parte del processo CI/CD.

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 È possibile utilizzare il driver di FireLens registro anziché il driver di 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 i parametri dei contenitori personalizzati 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 AWS 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. Impostare State Manager e Distributore per CloudWatch distribuzione e configurazione dell'agente

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 AWS Secrets Manager 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 integra con CloudWatch Registri per il piano di controllo Kubernetes. Il piano di controllo viene fornito come servizio gestito da Amazon EKS e puoiattiva la registrazione senza installare un agente CloudWatch. La CloudWatch agente può anche essere distribuito per acquisire i log dei nodi e dei container Amazon EKS. Fluent Bit e Fluentdsono supportati anche per l'invio dei registri dei container a CloudWatch registri.

CloudWatch Container Insights fornisce una soluzione completa di monitoraggio delle parametri per Amazon EKS a livello di cluster, nodo, pod, attività e servizio. Amazon EKS supporta anche più opzioni per l'acquisizione di metriche conPrometheus. Il piano di controllo Amazon EKS;fornisce un endpoint delle metricheche espone le metriche in un formato Prometheus. Puoi distribuire Prometheus nel tuo cluster Amazon EKS per utilizzare queste metriche.

Puoi ancheconfigurare CloudWatch Agente per lo scraping dei parametri Prometheuse crea CloudWatch metriche, oltre a consumare altri endpoint Prometheus. Monitoraggio di Container Insights per Prometheusè inoltre in grado di rilevare e acquisire automaticamente le metriche Prometheus da carichi di lavoro e sistemi supportati e containerizzati.

È possibile installare e configurare 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 Kubernetes può essere suddivisa in registrazione del piano di controllo, registrazione dei nodi e registrazione delle applicazioni. LaPiano di controllo Kubernetesè un insieme di componenti che gestiscono i cluster Kubernetes e producono i log utilizzati per scopi di controllo e diagnostica. Con Amazon EKS puoiaccendere i registri per diversi componenti del piano di controlloe inviali 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 ed è possibile configurare CloudWatch e Container Insights per acquisire questi log per ogni nodo Amazon EKS.

I contenitori sono raggruppati comebaccelliall'interno di un cluster Kubernetes e sono pianificati per l'esecuzione sui nodi Kubernetes. La maggior parte delle applicazioni containerizzate scrive su output

standard e errore standard e il motore contenitore reindirizza l'output a un driver di registrazione. In Kubernetes, i registri dei contenitori si trovano nella`/var/log/pods`directory su un nodo. È possibile configurare CloudWatch e Container Insights per acquisire questi registri per ciascuno dei tuoi pod Amazon EKS.

Registrazione 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 daAWS. 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 sono forniti per ogni istanza del componente del piano di controllo Kubernetes.AWSgestisce lo stato dei nodi del piano di controllo e fornisce unService Level Agreement (SLA) per l'endpoint Kubernetes.

Registrazione di nodo e applicazioni Amazon EKS

Ti consigliamo di utilizzareCloudWatch Container Insightsper acquisire registri e metriche per Amazon EKS. Container Insights implementa metriche a livello di cluster, nodo e pod con CloudWatch agent e Fluent Bit o Fluentd per l'acquisizione di log su CloudWatch. Container Insights fornisce anche dashboard automatici con viste a più livelli delle immagini acquisite CloudWatch Parametri di Container Insights viene distribuito come CloudWatch DaemonSet e Fluent Bit DaemonSet che funziona su tutti i nodi Amazon EKS. I nodi Fargate non sono supportati da Container Insights perché i nodi sono gestiti daAWSe non supporta DaemonSets. La registrazione di Fargate per Amazon EKS è coperta separatamente in questa guida.

La tabella riportata di seguito mostra CloudWatch gruppi di log e log acquisiti dalconfigurazione predefinita dell'acquisizione di log Fluentd o Fluent Bitper Amazon EKS.

`/aws/containerinsights/Cluster_Name/application`	Tutti i file di log in`/var/log/containers` . Questa directory fornisce collegamenti simbolici a tutti i registri del contenitore Kubernetes nella`/var/log/pods` Struttura delle directory . In questo modo vengono acquisiti i

	registri del contenitore dell'applicazione per scriverestdoutostderr. Include anche i registri per i contenitori di sistema Kubernetes comeaws-vpc-cni-init,kube-proxy , ecoreDNS.
/aws/containerinsights/Cluster_Name/host	I log da/var/log/dmesg ,/var/log/secure , e/var/log/messages .
/aws/containerinsights/Cluster_Name/dataplane	I log in /var/log/journal per kubelet.service kubeproxy .service e docker.service .

Se non si desidera utilizzare Container Insights con Fluent Bit o Fluentd per la registrazione, è possibile acquisire i log dei nodi e dei contenitori con CloudWatch Agente installato sui nodi Amazon EKS. I nodi Amazon EKS sono istanze EC2, il che significa che dovresti includerli nel tuo approccio di registrazione a livello di sistema standard per Amazon EC2. Se si installa il CloudWatch agente che utilizza Distributor e State Manager, quindi i nodi Amazon EKS sono inclusi anche nel CloudWatch installazione, configurazione e aggiornamento dell'agente.

La tabella seguente mostra i registri specifici di Kubernetes e che è necessario acquisire se non si utilizza Container Insights con Fluent Bit o Fluentd per la registrazione.

/var/log/containers	Questa directory fornisce collegamenti simbolici a tutti i registri del contenitore Kubernetes sotto/var/log/pods Struttura delle directory . In questo modo è possibile acquisire in modo efficace i registri del contenitore dell'appl icazionestdoutostderr. Ciò include i registri per i contenitori di sistema Kubernetes comeaws-vpc-cni-init ,kube-proxy , ecoreDNS. Importante: Questo non è necessari o se si utilizza Container Insights.
var/log/aws-routed-eni/ipamd.log	I registri per il demone L-IPAM sono disponibili qui

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

È necessario assicurarsi che i nodi Amazon EKS installino e configurino il CloudWatch agente per inviare log e metriche a livello di sistema appropriati. Tuttavia, l'AMI ottimizzato di Amazon EKS non include l'agente di Systems Manager. Utilizzandomodelli di avvio, è possibile automatizzare l'installazione dell'agente di Systems Manager e un'impostazione predefinita CloudWatch configurazione che acquisisce importanti registri specifici di Amazon EKS con uno script di avvio implementato attraverso la sezione dati utente. I nodi Amazon EKS vengono distribuiti utilizzando un gruppo Auto Scaling comegruppo di nodi gestitio comenodi autogestiti.

Con i gruppi di nodi gestiti, fornisci unmodello di avvioche include la sezione dati utente per automatizzare l'installazione dell'agente di Systems Manager e CloudWatch Configurazione di È possibile personalizzare e utilizzare ilamazon_eks_managed_node_group_launch_config.yaml AWS CloudFormationmodello per creare un modello di lancio che installa l'agente Systems Manager, CloudWatch agente e aggiunge anche una configurazione di registrazione specifica di Amazon EKS al CloudWatch directory di configurazione. Questo modello può essere utilizzato per aggiornare il modello di avvio dei gruppi di nodi gestiti Amazon EKS con un infrastructure-as-code Approccio (iAC). Ogni aggiornamento delAWS CloudFormationfornisce una nuova versione del modello di lancio. Quindi puoi aggiornare il gruppo di nodi per utilizzare la nuova versione del modello e disporre diprocesso del ciclo di vita gestitoaggiorna i nodi senza tempi di inattività. Assicurati che il ruolo IAM e il profilo di istanza applicati al gruppo di nodi gestiti includano il`CloudWatchAgentServerPolicy`e`AmazonSSMManagedInstanceCore` AWSpolicy gestite.

Con i nodi autogestiti, esegui direttamente il provisioning e la gestione del 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 eBottlerocket, insieme aaltre opzioni. È possibile utilizzareAWS CloudFormationper distribuire nodi autogestiti nei cluster Amazon EKS, il che significa che puoi utilizzare un approccio IAC e di modifica gestita per i cluster Amazon EKS.AWSfornisce il softwareamazon-eks-nodegroup.yaml AWS CloudFormationmodello che puoi utilizzare così come è o personalizzabile. Il modello fornisce tutte le risorse richieste per i nodi Amazon EKS in un cluster (ad esempio, un ruolo IAM separato, un gruppo di sicurezza, un gruppo di Amazon EC2 Auto Scaling e un modello di avvio). Laamazon-eks-nodegroup.yaml AWS CloudFormationtemplate è una versione aggiornata che installa l'agente di Systems Manager richiesto, CloudWatch agente e aggiunge anche una configurazione di registrazione specifica di Amazon EKS al CloudWatch directory di configurazione.

Registrazione per Amazon EKS su Fargate

Con Amazon EKS su Fargate, puoi distribuire pod senza allocare o gestire i nodi Kubernetes. Ciò elimina la necessità di acquisire registri a livello di sistema per i nodi Kubernetes. Per catturare i registri dai tuoi pod Fargate, puoi usare Fluent Bit per inoltrare i log direttamente a CloudWatch. Ciò consente di instradare automaticamente i log a CloudWatch senza ulteriore configurazione o un contenitore sidecar per i tuoi pod Amazon EKS su Fargate. Per ulteriori informazioni, consultaRegistrazione Fargatenella documentazione di Amazon EKS eFluent Bit per Amazon EKSsulAWSBlog. Questa soluzione cattura il`STDOUT`e`STDERR`input/output (I/O) trasmette dal contenitore e li invia a CloudWatch tramite Fluent Bit, basato sulla configurazione Fluent Bit stabilita per il cluster Amazon EKS su Fargate.

Parametri per Amazon EKS e Kubernetes

Kubernetes fornisce un'API delle metriche che consente di accedere alle metriche di utilizzo delle risorse (ad esempio, utilizzo di CPU e memoria per nodi e pod), ma l'API fornisce solo informazioni point-in-time e non metriche cronologiche. LaMetric-server Kubernetesviene solitamente utilizzato per le distribuzioni di Amazon EKS e Kubernetes per aggregare le metriche, fornire informazioni cronologiche a breve termine sulle metriche e supportare funzionalità comeHorizontal Pod Autoscaler.

Amazon EKS espone le metriche del piano di controllo tramite il server API Kubernetesin formato Prometheuse CloudWatch è in grado di acquisire e acquisire queste metriche. CloudWatch e Container Insights possono anche essere configurati per fornire l'acquisizione, l'analisi e l'allarmamento di metriche complete per i nodi e i pod Amazon EKS.

Parametri del piano di controllo Kubernetes

Kubernetes espone le metriche del piano di controllo in un formato Prometheus utilizzando il`/metrics`Endpoint API HTTP. È consigliabile installarePrometheusnel cluster Kubernetes per graficare e visualizzare queste metriche con un browser Web. Puoi ancheacquisisci le metriche esposteda server API Kubernetes in CloudWatch.

Metriche di nodi e di sistema per Kubernetes

Kubernetes fornisce il Prometheusmetrics-serverpod che puoidistribuisci ed eseguisui cluster Kubernetes per le statistiche di CPU e memoria a livello di cluster, nodo e pod. Queste metriche

vengono utilizzate con ilHorizontal Pod AutoscalereVertical Pod Autoscaler. CloudWatch può anche fornire queste metriche.

È necessario installare Kubernetes Metrics Server se si utilizza ilPannello di controllo Kubernetesо gli autoscaler orizzontali e verticali. Kubernetes Dashboard consente di sfogliare e configurare il cluster Kubernetes, i nodi, i pod e la relativa configurazione e visualizzare le metriche della CPU e della memoria dal Kubernetes Metrics Server. È possibile distribuire questa soluzione per singoli cluster seguendo la procedura descritta nella sezioneDistribuzione del pannello di controllo Kubernetesnella documentazione di Amazon EKS.

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

Container Insights utilizza una versione containerizzata del CloudWatch agente che funziona in un Kubernetes DaemonSet per scoprire tutti i contenitori in esecuzione in un cluster e fornire metriche a livello di nodo. Raccoglie i dati sulle prestazioni a ogni livello dello stack delle prestazioni. È possibile utilizzare il Quick Start daAWSAvvia rapida o configurazione di Container Insights separatamente. Il Quick Start consente di configurare il monitoraggio delle metriche con CloudWatch agente e logging con Fluent Bit, quindi è necessario distribuirlo una sola volta per la registrazione e il monitoraggio.

Poiché i nodi Amazon EKS sono istanze EC2, è necessario acquisire metriche a livello di sistema, oltre alle metriche acquisite da Container Insights, utilizzando gli standard definiti per Amazon EC2. È possibile utilizzare lo stesso approccio dalImpostare State Manager e Distributore per CloudWatch distribuzione e configurazione dell'agentesezione di questa guida per installare e configurare CloudWatch Agente per i cluster Amazon EKS. Puoi aggiornare il tuo file di configurazione CloudWatch specifico di Amazon EKS per includere le metriche e la configurazione di log specifica di Amazon EKS.

La CloudWatch agente con supporto Prometheus può scoprire e raschiare automaticamente le metriche di Prometheuscarichi di lavoro e sistemi supportati e containerizzati. Li ingerisce come CloudWatch accede al formato metrico incorporato per l'analisi con CloudWatch Registra Insights e crea automaticamente le metriche di CloudWatch.

> **Important**
>
> Devi essere presenteimplementare una versione specializzatadel CloudWatch per raccogliere le metriche Prometheus. Questo è un agente distinto dal CloudWatch Agente distribuito per

Container Insights. Puoi utilizzare il pluginprometheus_jmxapplicazione Java di esempio, che include i file di distribuzione e configurazione per CloudWatch implementazione dell'agente e del pod Amazon EKS per dimostrare il rilevamento delle metriche di Prometheus. Per ulteriori informazioni, consultaConfigurazione del carico di lavoro di esempio Java/JMX su Amazon EKS e Kubernetesnella documentazione di CloudWatch. È anche possibile configurare CloudWatch agente per acquisire metriche da altri target Prometheus in esecuzione nel cluster Amazon EKS.

Parametri di applicazione

Puoi creare parametri personalizzati conFormato metrico incorporato CloudWatch. Per acquisire istruzioni di formato metrico incorporato, è necessario inviare voci di formato metrico incorporato a un endpoint del formato metrico incorporato. La CloudWatch agente può essere configurato comecontenitore sidecar nel tuo pod Amazon EKS. La CloudWatch la configurazione dell'agente è memorizzata come Kubernetes ConfigMap e letto dal tuo CloudWatch container agente sidecar per avviare l'endpoint del formato metrico incorporato.

Puoi anche configurare l'applicazione come target Prometheus e configurare l'agente CloudWatch, con il supporto Prometheus, per scoprire, raschiare e acquisire le tue metriche in CloudWatch. Ad esempio, è possibile utilizzare il softwareesportatore JMX open sourcecon le tue applicazioni Java per esporre JMX Beans per il consumo di Prometheus da parte del CloudWatch agente.

Se non vuoi utilizzare il formato metrico incorporato, puoi anche creare e aggiornare le metriche di CloudWatch utilizzandoAWSAPIoAWS SDK. Tuttavia, lo sconsigliamo 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 metriche a livello di nodo. Tuttavia, devi monitorare le metriche per i pod in esecuzione sui tuoi nodi Amazon EKS su Fargate. Container Insights non è attualmente disponibile per Amazon EKS su Fargate perché richiede le seguenti funzionalità attualmente non supportate:

- DaemonSets non sono attualmente supportati. Container Insights viene distribuito eseguendo il CloudWatch come agente come DaemonSet su ciascun nodo cluster.

- I volumi persistenti di HostPath non sono supportati. La CloudWatch agent container utilizza i volumi persistenti HostPath come prerequisito per la raccolta dei dati metrici del contenitore.
- Fargate impedisce ai container privilegiati e l'accesso alle informazioni sull'host.

Puoi utilizzare il pluginrouter di log integrato per Fargateper inviare istruzioni di formato metrico incorporato a CloudWatch. Il router di log utilizza Fluent Bit, che ha un CloudWatch plugin che può essere configurato per supportare istruzioni di formato metrico incorporato.

Puoi recuperare e acquisire metriche a livello di pod per i tuoi nodi Fargate distribuendo il server Prometheus nel cluster Amazon EKS per raccogliere le metriche dai 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, consultaMonitoraggio di Amazon EKSAWS Fargateusando Prometheus e GrafanasulAWSBlog.

Monitoraggio Prometheus su Amazon EKS

Amazon Managed Service for Prometheusfornisce una soluzione scalabile, sicura,AWSservizio gestito per Prometheus open-source. È possibile utilizzare Prometheus Query Language (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 le metriche Prometheus da Amazon EKS e Amazon ECS utilizzandoAWSDistro per OpenTelemetry (ADULTO)o server Prometheus come agenti di raccolta.

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

- Amazon Managed Service for Prometheus consente di utilizzare i server Prometheus esistenti distribuiti in Amazon EKS o Kubernetes autogestiti e configurarli per scrivere su Amazon Managed Service per Prometheus anziché in un data store configurato localmente. In questo modo si eliminano i carichi pesanti indifferenziati della gestione di un data store altamente disponibile per i server Prometheus e la sua infrastruttura. Amazon Managed Service per Prometheus è una scelta adatta quando si dispone di una distribuzione di Prometheus matura che si desidera sfruttare nelAWSCloud.
- Grafana supporta direttamente Prometheus come fonte di dati per la visualizzazione. Se vuoi usare Grafana con Prometheus invece di CloudWatch Dashboard per il monitoraggio dei container, quindi Amazon Managed Service per Prometheus potrebbe soddisfare le tue esigenze. Amazon Managed Service per 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,lo CloudWatch l'agente ingesta parametri Prometheus in Embedded Metric Formatdentro CloudWatch Registri che hanno come risultato CloudWatch Parametri di È possibile eseguire query sui log in Embedded Metric Format utilizzando CloudWatch Log Insights.
- Se non disponi di utilizzare CloudWatch per il monitoraggio e l'acquisizione delle metriche, è necessario utilizzare Amazon Managed Service per Prometheus con il server Prometheus e una soluzione di visualizzazione come Grafana. È necessario configurare il server Prometheus per raschiare le metriche dai target Prometheus e configurare il server inscrittura remota sul

tuo workspace su Amazon Managed Service for Prometheus. Se utilizzi Amazon Managed Grafana, puoiintegra direttamente Amazon Managed Grafana con la tua origine dati Amazon Managed Service per Prometheus utilizzando il plugin incluso. Poiché i dati delle metriche sono archiviati in Amazon Managed Service per Prometheus, non esiste alcuna dipendenza da distribuire CloudWatch agente o requisito per l'acquisizione di dati in CloudWatch. La CloudWatch è necessario per il monitoraggio di Container Insights for Prometheus.

Puoi anche utilizzare ADOT Collector per raschiare da un'applicazione strumentata da Prometheus e inviare le metriche ad Amazon Managed Service for Prometheus. Per ulteriori informazioni su ADOT Collector, consulta laAWSDistro for OpenTelemetrydocumentazione.

Registrazione e metriche perAWS Lambda

Lambdaelimina la necessità di gestire e monitorare i server per i carichi di lavoro e funziona automaticamente con CloudWatchMetriche e CloudWatch Registra i log senza ulteriore configurazione o strumentazione del codice dell'applicazione. Questa sezione ti aiuta a comprendere le caratteristiche prestazionali dei sistemi utilizzati da Lambda e in che modo 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 i messaggi di output standard e di errore standard da una funzione Lambda a CloudWatch Registra, senza richiedere la registrazione dei driver. 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 la chiamata 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 e si trova in`/aws/lambda/<YourLambdaFunctionName>`formato. Nel gruppo di log viene creato un flusso di log separato per ogni istanza della funzione Lambda. Lambda ha una convenzione di denominazione standard per i flussi di log che utilizza un`YYYY/MM/DD/[<FunctionVersion>]<InstanceId>`formato. Il`InstanceId`è generato daAWSper 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 ilModulo di registrazione Pythonper 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 ilAWSLambda Powertools per Pythontoolkit per sviluppatori che semplifica l'arricchimento dei messaggi di log con dati chiave come gli avviamenti 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 delle funzioni Lambda senza aggiornare il codice. Ad esempio, puoi creare un`LAMBDA_LOG_LEVEL`variabile di ambiente che definisce il livello di output del registro che è possibile recuperare dal codice. L'esempio seguente tenta di recuperare un`LAMBDA_LOG_LEVEL`variabile di ambiente e utilizza il valore per definire l'output di registrazione. Se la variabile di ambiente non è impostata, il valore predefinito è`INFO`livello.

```
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 Servizio o una funzione Lambda) utilizzando i filtri di abbonamento. Se non utilizzi Amazon OpenSearch Servizio, puoi utilizzare una funzione Lambda per elaborare i log e inviarli a unAWSservizio di tua scelta utilizzando ilAWSSDK.

Puoi anche utilizzare gli SDK per destinazioni di log al di fuori diAWSInserisci nel cloud la 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, il tempo di elaborazione aggiuntivo, la gestione degli errori e dei tentativi e l'abbinamento 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 delle verifiche 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 rendere l'acquisizione a livello di applicazione CloudWatch metriche più semplici.

Metriche a livello di sistema

Lambda si integra automaticamente con CloudWatch Metrica e fornisce una serie dimetriche 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 consente di diagnosticare e supportare le implementazioni Lambda.

Errori di invocazioneimpedisci 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. Dovresti invece 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`Errors`la metrica acquisisce e identifica 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 forniscCloudWatch Lambda Insightsche puoi abilitare per una singola funzione Lambda. Lambda Insights raccoglie, aggrega e riepiloga le metriche a livello di sistema (ad esempio,

tempo della 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 dei lavoratori Lambda) per aiutarti a isolare e risolvere rapidamente i problemi.

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

Parametri di applicazione

Puoi anche creare e acquisire le metriche delle tue applicazioni in CloudWatch utilizzando il formato metrico incorporato. Puoi sfruttareAWS ha fornito librerie per il formato metrico incorporatoper creare ed emettere istruzioni in formato metrico incorporato per CloudWatch. La Lambda integrata CloudWatch la struttura di registrazione 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, è possibile 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 registri. La maggior parte dei carichi di lavoro utilizza una raccolta diAWS risorse come rete, elaborazione, storage e database. Ove possibile, è necessario analizzare collettivamente le metriche e i log di queste risorse e correlarli per monitorare e gestire efficacemente tutti iAWS carichi di lavoro.

CloudWatch offre diverse funzionalità per aiutare ad analizzare registri e metriche, come CloudWatch Application Insights per definire e monitorare collettivamente metriche e registri per un'applicazione suAWS risorse diverse, CloudWatch Anomaly Detection per individuare le anomalie per le tue metriche e CloudWatch Log Insights per eseguire ricerche interattive e analizzare i dati di registro in CloudWatch Logs.

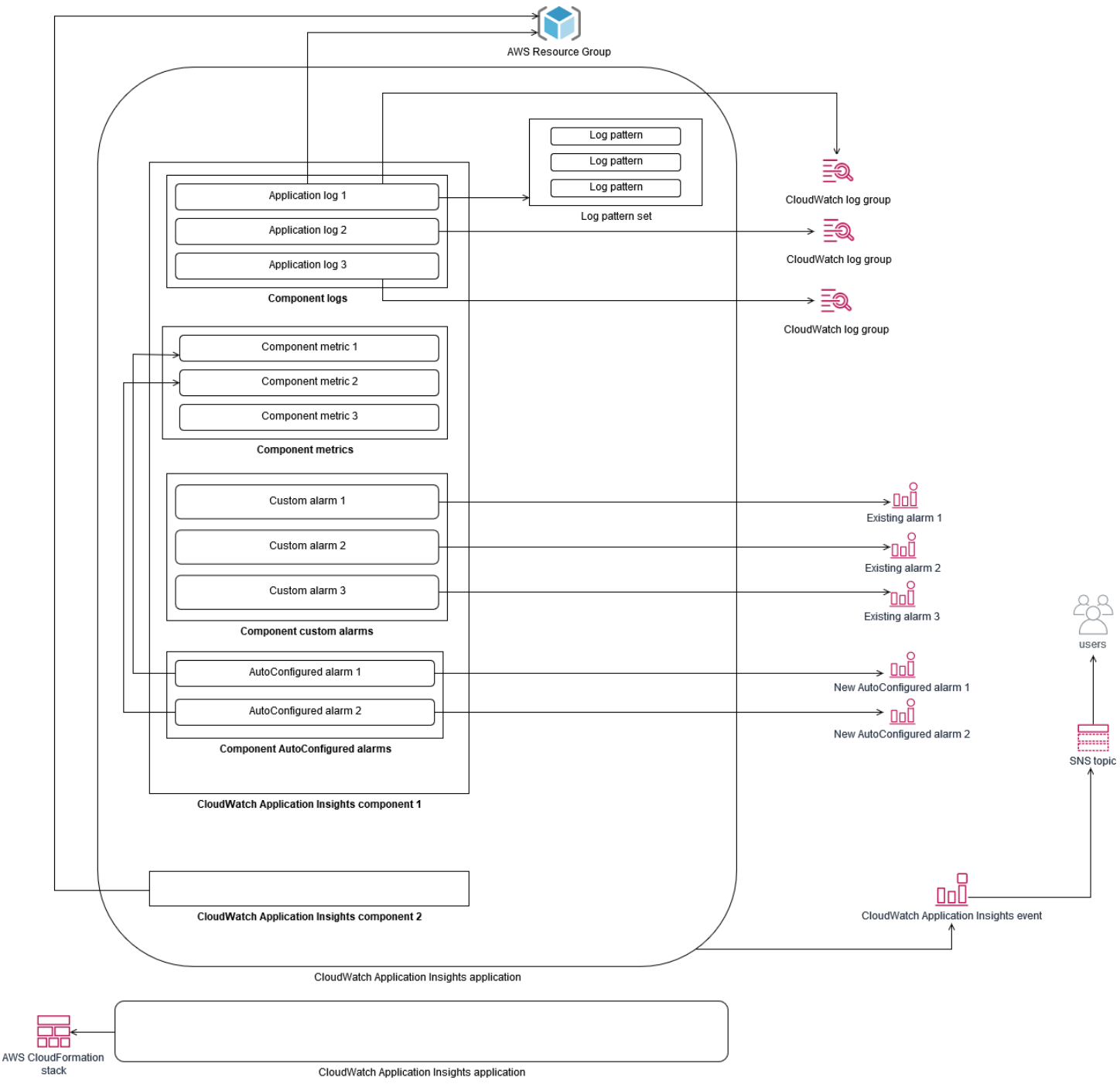
Monitora e analizza collettivamente le applicazioni con CloudWatch Application Insights

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 CloudWatch dell'applicazione Application Insights. Un set di pattern di log è una raccolta di pattern di log

da cercare in base a espressioni regolari, insieme a una gravità bassa, media o alta quando 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 CloudWatch Application Insights nella CloudWatch documentazione. 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 registri e metriche da monitorare utilizzando CloudWatch registri e metriche.



Le istanze EC2 monitorate da CloudWatch Application Insights richiedono Systems Manager, CloudWatch agenti e autorizzazioni. Per ulteriori informazioni a riguardo, vedere Prerequisiti per configurare un'applicazione con CloudWatch Application Insights nella CloudWatch documentazione. 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 di Systems Manager con

ilAmazonCloudWatch-ApplicationInsights-SSMParameter prefisso per ogni componente di CloudWatch Application Insights. Ciò comporta l'aggiunta di un file di configurazione dell' CloudWatch agente separato alla directory di configurazione dell' CloudWatch agente sull'istanza EC2. Viene eseguito un comando di Systems Manager per aggiungere questa configurazione alla configurazione attiva sull'istanza EC2. CloudWatch L'utilizzo di Application Insights non influisce sulle impostazioni di configurazione degli CloudWatch agenti esistenti. È possibile utilizzare CloudWatch Application Insights in aggiunta alle proprie configurazioni di CloudWatch agenti a livello di sistema e applicazione. Tuttavia, dovresti assicurarti 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 individua automaticamente i campi JSON nei flussi di log in più gruppi di log. È possibile utilizzare CloudWatch Logs Insights per analizzare i log delle applicazioni e del sistema, salvando le query per un uso future. La sintassi delle 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 usi il formato metrico incorporato per creare CloudWatch metriche, puoi interrogare i registri del formato metrico incorporato per generare metriche monouso utilizzando le funzioni di aggregazione supportate. Ciò consente di ridurre i costi di CloudWatch monitoraggio acquisendo i 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 comporterebbero 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 dai dati della metrica acquisiti nell'istruzione in formato metrico incorporato:

```
{
 "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, puoi eseguire la query seguente 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 CloudWatch registro dai gruppi di log a un cluster Amazon OpenSearch Service di tua scelta con un filtro di abbonamento. Puoi utilizzarlo CloudWatch per l'acquisizione e l'analisi dei log e delle metriche primari e quindi ampliarlo 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 di campo e aiuta a rendere anonimi i dati nei campi in base alle

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

- Aggrega e cerca i log di più account, regioni e infrastrutture: puoi trasmettere i tuoi log da più account e regioni in un cluster Amazon OpenSearch Service comune. I tuoi team operativi centralizzati possono analizzare tendenze, problemi ed eseguire analisi su account e regioni. Lo streaming CloudWatch dei log su Amazon OpenSearch Service consente inoltre di 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 possono utilizzare sistemi operativi non supportati dall' CloudWatch agente. Potresti anche voler arricchire e trasformare i dati di registro prima che vengano spediti alla tua soluzione di registrazione. Amazon OpenSearch Service supporta client Elasticsearch standard come gli spedizionieri di dati della famiglia Elastic Beats e Logstash che supportano l'arricchimento e la trasformazione dei log prima dell'invio dei dati di registro ad Amazon OpenSearch Service.
- La soluzione di gestione delle operazioni esistente utilizza uno ElasticSearchstack 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 delle dashboard operative create in Kibana che desideri continuare a utilizzare.

Se non prevedi di utilizzare CloudWatch i log, puoi utilizzare agenti, driver di registro e librerie supportati da Amazon OpenSearch Service (ad esempio, Fluent Bit, Fluentd, logstash e Open Distro for ElasticSearch API) per spedire i tuoi log direttamente ad Amazon OpenSearch Service e bypassarli CloudWatch. Tuttavia, dovresti anche implementare una soluzione per acquisire i log generati daiAWS servizi. CloudWatch Logs è la soluzione di acquisizione dei log principale per moltiAWS 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 impostare un filtro di abbonamento per un gruppo di log per lo streaming dei relativi log su 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, è possibile implementare una soluzione che sottoscrive automaticamente nuovi gruppi di log ai ElasticSearch cluster. Puoi trasmettere i log a un ElasticSearch cluster nello stesso account o in 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 considerare la possibilità di configurare un ElasticSearch cluster in un account centralizzato o condiviso per aggregare i log tra i tuoi account, regioni e applicazioni. Ad esempio,AWS Control Tower imposta un account Log Archive che viene utilizzato per la registrazione centralizzata. Quando viene creato un nuovo accountAWS Control Tower, i relativiAWS CloudTrailAWS Config registri vengono inviati a un bucket S3 in questo account centralizzato. La registrazione strumentata daAWS Control Tower è per la configurazione, le modifiche e la registrazione di audit.

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

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 consente di ridurre il rischio 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 automatica e automatica di metriche importanti consente di rilevare e risolvere i problemi prima che influiscano sui carichi di lavoro. CloudWatch semplifica il grafico e il confronto di più metriche utilizzando più statistiche in un determinato periodo di tempo. È possibile utilizzare CloudWatch per cercare tra tutte le metriche con i valori di dimensione richiesti per trovare le metriche necessarie per l'analisi.

Si consiglia 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 corso del tempo, il carico di lavoro matura e puoi aggiungere ulteriori metriche e dimensioni per aiutarti a analizzarlo e supportarlo ulteriormente. Le applicazioni o i carichi di lavoro potrebbero utilizzarne piùAWSrisorse e avere metriche personalizzate, è necessario raggruppare queste risorse in uno spazio dei nomi per renderle più facili da identificare.

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 utilizzareServiceLens CloudWatchper correlare tracce, metriche, registri e allarmi per la diagnosi dei problemi. È inoltre consigliabile includere dimensioni aggiuntive nelle metriche e negli identificatori nei registri per i carichi di lavoro per aiutarti a cercare e identificare rapidamente i problemi tra i sistemi e i servizi.

Utilizzo di CloudWatch allarmi per il monitoraggio e allarmi

È possibile utilizzareAllarmi CloudWatchper ridurre il monitoraggio manuale dei carichi di lavoro o delle applicazioni. È necessario iniziare esaminando le metriche acquisite per ciascun componente del carico di lavoro e determinando le soglie appropriate per ogni metrica. Assicurati di identificare quali membri del team devono essere avvisati quando viene violata una soglia. È necessario stabilire e indirizzare i gruppi di distribuzione, anziché i singoli membri del team.

Gli allarmi CloudWatch possono integrarsi con la soluzione di gestione dei servizi per creare automaticamente nuovi ticket ed eseguire flussi di lavoro operativi. Ad esempio:AWSfornisce ilAWSService Management Connector perServiceNoweDesk di assistenza Jiraper aiutarti a configurare rapidamente le integrazioni. Questo approccio è fondamentale per garantire che gli allarmi sollevati siano riconosciuti e allineati ai flussi di lavoro operativi esistenti che potrebbero già essere definiti in questi prodotti.

È inoltre possibile 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, in presenza di`OrderQueueDepth`metrica che tiene traccia degli ordini dei clienti, è possibile definire una soglia inferiore in un breve periodo medio di un minuto che notifica i membri del team dell'applicazione via e-mail oRallentamento. È inoltre possibile definire un altro allarme per la stessa metrica per un periodo di 15 minuti più lungo alla stessa soglia e che pagine, e-mail e notifica al team di applicazione e al lead del team di applicazione. Infine, è possibile definire un terzo allarme per una soglia media rigida per un periodo di 30 minuti che notifica la gestione superiore e notifica a tutti i membri del team precedentemente notificati. La creazione di più allarmi consente di intraprendere azioni diverse per le diverse condizioni. È possibile iniziare con un semplice processo di notifica e quindi modificarlo e migliorarlo secondo necessità.

Utilizzo di CloudWatch rilevamento di anomalie da monitorare e allarme

È possibile utilizzareRilevazione delle anomalie di Cloudse non si è sicuri delle soglie da applicare per una determinata metrica o se si desidera che un allarme regola automaticamente i valori di soglia in base ai valori storici osservati. CloudWatch il rilevamento delle anomalie è particolarmente utile per le metriche che potrebbero presentare cambiamenti regolari e prevedibili nell'attività, ad esempio gli ordini di acquisto giornalieri per la consegna nello stesso giorno aumentano prima di un orario limite. Il rilevamento delle anomalie consente soglie che si regolano automaticamente e possono contribuire a ridurre i falsi allarmi. È possibile abilitare il rilevamento delle anomalie per ogni metrica e statistica e configurare CloudWatch all'allarme basato su valori anomali.

Ad esempio, è possibile abilitare il rilevamento delle anomalie per il`CPUUtilization`metrica e`AVG`statistica su un'istanza EC2. 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 escalation degli allarmi, in modo simile alla creazione di più allarmi standard con soglie diverse.

Per ulteriori informazioni su questa sezione, consultaCreazione di un allarme CloudWatch basato sul rilevamento di anomalienella CloudWatch documentazione.

Alarmante per più regioni e account

I proprietari di applicazioni e carichi di lavoro devono creare allarmi a livello di applicazione per carichi di lavoro che abbracciano più regioni. Si consiglia di creare allarmi separati all'interno di ciascun

account e regione in cui è stato distribuito il carico di lavoro. È possibile semplificare e automatizzare questo processo utilizzando account e Region agnosticAWS CloudFormation StackSets e modelli per distribuire le risorse applicative con gli allarmi richiesti. modelloÈ possibile configurare le azioni di allarme per indirizzare un argomento comune Amazon Simple Notification Service (Amazon SNS), il che significa che la stessa azione di notifica o correzione viene utilizzata indipendentemente dall'account o dalla regione.

Negli ambienti multi-account e multi-regione, ti consigliamo di creare allarmi aggregati per i tuoi account e le regioni per monitorare i problemi relativi all'account e alle aree regionali utilizzandoAWS CloudFormation StackSets e metriche aggregate, come la media`CPUUtilization`in tutte le istanze EC2.

Si consiglia inoltre di creare allarmi standard per ogni carico di lavoro configurato per lo standard CloudWatch metriche e registri acquisiti. Ad esempio, è possibile creare un allarme separato per ogni istanza EC2 che monitora la metrica di utilizzo della CPU e notifica a un team operativo centrale quando l'utilizzo medio della CPU è superiore all'80% su base giornaliera. È inoltre possibile creare un allarme standard che monitora l'utilizzo medio della CPU inferiore al 10% su base giornaliera. Questi allarmi aiutano il team operativo centrale a lavorare con specifici proprietari di carichi di lavoro per modificare le dimensioni delle istanze EC2 quando necessario.

Automatizzazione della creazione di allarmi con tag di istanza EC2

La creazione di un set standard di allarmi per le istanze EC2 può richiedere molto tempo, incoerente e soggetta a errori. È possibile accelerare il processo di creazione degli allarmi utilizzando ilamazon-cloudwatch - allarmi automaticisoluzione per creare automaticamente un set standard di allarmi CloudWatch per le istanze EC2 e creare allarmi personalizzati basati su tag di istanza 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. È inoltre possibile distribuire questa soluzione conAWS CloudFormation StackSets per supportare più regioni e account. Per ulteriori informazioni, consultaUsa i tag per creare e gestire Amazon CloudWatch allarmi per istanze Amazon EC2sulAWSBlog.

Monitoraggio della disponibilità di applicazioni e servizi

CloudWatch ti aiuta a monitorare e analizzare le prestazioni e gli aspetti di runtime delle applicazioni e dei carichi di lavoro. È inoltre necessario monitorare gli aspetti di disponibilità e raggiungibilità delle applicazioni e dei carichi di lavoro. È possibile ottenere questo risultato utilizzando un approccio di monitoraggio attivoControllo dello stato di Amazon Route 53eCloudWatch Synthetics.

È possibile utilizzare i controlli dello stato di Route 53 quando si desidera monitorare la connettività a una pagina Web tramite HTTP o HTTPS o la connettività di rete tramite TCP a un nome DNS (Domain Name System) pubblico o indirizzo IP. I controlli dello stato di Route 53 avviano le connessioni dalle Regioni specificate a intervalli di dieci o 30 secondi. È possibile scegliere più regioni in cui eseguire il controllo dello stato, ogni controllo dello stato viene eseguito in modo indipendente ed è necessario scegliere almeno tre regioni. È possibile cercare nel corpo di risposta di una richiesta HTTP o HTTPS una sottostringa specifica se appare nei primi 5.120 byte di dati restituiti per la valutazione del controllo dello stato. Una richiesta HTTP o HTTPS è considerata integra se restituisce una risposta 2xx o 3xx. I controlli dello stato di Route 53 possono essere utilizzati per creare un controllo dello stato composito controllando lo stato di altri controlli sanitari. È possibile farlo se si dispone di più endpoint del servizio e si desidera eseguire la stessa notifica quando uno di essi diventa malsano. Se si utilizza Route 53 per DNS, è possibile configurare Route 53 infailover su un'altra voce DNSse un controllo dello stato diventa malsano. Per ogni carico di lavoro critico, è consigliabile impostare i controlli dello stato di Route 53 per gli endpoint esterni critici per le normali operazioni. I controlli dello stato di Route 53 consentono di evitare di scrivere la logica di failover nelle applicazioni.

CloudWatch synthetics consente di definire un canarino come script per valutare lo stato e la disponibilità dei carichi di lavoro. I canary 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. Ciascun canarino definito può eseguire più chiamate HTTP o HTTPS su endpoint diversi. Ciò significa che è possibile monitorare lo stato di una serie di passaggi, come un caso d'uso o un endpoint con dipendenze a valle. Creare un canary CloudWatch metriche che includono ogni passaggio eseguito in modo da poter allarmi e misurare i diversi passaggi in modo indipendente. Sebbene le canarine richiedano più pianificazione e impegno da sviluppare rispetto ai controlli sullo stato di Route 53, offrono un approccio di monitoraggio e valutazione altamente personalizzabile. Canaries supporta anche risorse private in esecuzione all'interno del cloud privato virtuale (VPC), il che le rende ideali per il monitoraggio della disponibilità quando non si dispone di un indirizzo IP pubblico per l'endpoint. È inoltre possibile utilizzare le canarie per monitorare i carichi di lavoro locali

a condizione che si disponga di connettività dall'interno del VPC all'endpoint. Ciò è particolarmente importante quando si dispone di un carico di lavoro che include endpoint esistenti in loco.

Applicazioni di tracciamento conAWS X-Ray

Una richiesta tramite l'applicazione potrebbe consistere in chiamate a database, applicazioni e servizi Web in esecuzione su server locali, Amazon EC2, container o Lambda. Implementando il trace delle applicazioni, è possibile identificare rapidamente la causa principale dei problemi nelle applicazioni che utilizzano componenti e servizi distribuiti. É possibile utilizzareAWS X-Rayper tracciare le richieste dell'applicazione su più componenti. Campioni a X-Ray e visualizza le richieste su unGrafico del servizioquando scorrono 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 scorre attraverso più componenti, il che consente di visualizzare la richiesta da un punto all'altro. È possibile migliorarlo ulteriormente 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. Inoltre, X-Ray fornisceAWSSDK per più lingue, inclusi client strumentati che inviano automaticamente i dati a X-Ray. Gli SDK X-Ray forniscono patch alle librerie comuni utilizzate per effettuare chiamate ad altri servizi (ad esempio, HTTP, MySQL, PostgreSQL o MongoDB).

X-Ray fornisce un demone a raggi X che è possibile 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 i dati sulle prestazioni dai server e dai contenitori che eseguono il demone X-Ray che ha servito la richiesta. X-Ray controlla automaticamente le tue chiamateAWSservizi, come Amazon DynamoDB, come sottosegmenti tramite patchAWSSDK. X-Ray può anche integrarsi automaticamente con le funzioni Lambda.

Se i componenti dell'applicazione effettuano chiamate a servizi esterni che non sono in grado di configurare e installare il demone a X-Ray o lo strumento del codice, è possibile crearesottosegmenti per avvolgere le chiamate a servizi esterni. Correlazione X-Ray CloudWatch registri e metriche con le tracce dell'applicazione se si utilizza ilSDK AWS X-Ray per Java, il che significa che è possibile analizzare rapidamente le metriche e i registri correlati per le richieste.

Implementazione del daemon 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 dei microservizi. É possibile utilizzare unascript di dati utenteper distribuire il demone a X-Ray quando vengono eseguite il provisioning delle istanze EC2 oppure è possibile includerlo nel processo di compilazione AMI se si creano le proprie AMI. Ciò può essere particolarmente utile quando le istanze EC2 sono effimere.

È necessario utilizzare State Manager per assicurarsi che il demone a X-Ray sia installato in modo coerente sulle istanze EC2. Per Amazon EC2finestreistanze, è possibile utilizzare Systems ManagerAWS-Esegui il documento PowerShellScriptper eseguireScript Windowsche scarica e installa l'agente X-Ray. Per le istanze EC2 su Linux, è possibile utilizzare ilAWS-RunShellScript documento per eseguire lo script Linuxscarica e installa l'agente come servizio.

È possibile utilizzare Systems ManagerAWS-Esegui il documento RemoteScriptper eseguire lo script in un ambiente multi-account. Devi creare un bucket S3 accessibile da tutti i tuoi account e ti consigliamocreazione di un bucket S3 con una policy del bucket basata sull'organizzazionese utilizziAWS Organizations. Quindi si caricano gli script nel bucket S3, ma assicurati che il ruolo IAM per le istanze EC2 abbia il permesso di accedere al bucket e agli script.

È inoltre possibile configurare State Manager per associare gli script alle istanze EC2 in cui è installato l'agente X-Ray. Poiché tutte le istanze EC2 potrebbero non richiedere o utilizzare i X-Ray, è possibile scegliere come target l'associazione con i tag di istanza. Ad esempio, è possibile creare l'associazione di State Manager in base alla presenza di`InstallAWSXRayDaemonWindows`o`InstallAWSXRayDaemonLinux`tag.

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

È possibile distribuire ilDaemon X-Raycome contenitore sidecar per carichi di lavoro basati su container come Amazon ECS o Amazon EKS. I contenitori dell'applicazione possono quindi connettersi al container sidecar con il collegamento dei container se utilizzi Amazon ECS, oppure il contenitore può connettersi direttamente al contenitore sidecar su localhost se si utilizzaModalità di rete awsvpc.

Per Amazon EKS, puoi definire il demone a X-Ray nella definizione del pod dell'applicazione e quindi l'applicazione può connettersi al demone tramite localhost sulla porta contenitore specificata.

Configurazione di Lambda per tracciare le richieste su X-Ray

L'applicazione potrebbe includere chiamate alle funzioni Lambda. Non è necessario installare il daemon 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 ilAWS Management Consolee controllando ilTracciamento attivonella console X-Ray.

Per ulteriori operazioni di strumentazione è possibile combinare l'SDK X-Ray con la funzione Lambda per registrare le chiamate in uscita e aggiungere annotazioni o metadati.

Strumentazione delle applicazioni per X-Ray

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

Quando si strumenta la tua applicazione, assicurati di creare annotazioni per aiutarti a identificare e cercare le richieste. Ad esempio, la tua applicazione potrebbe utilizzare un identificatore per i clienti, come`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 metadati contenente uno o più campi purché il documento del segmento non superi i 64 kilobyte. È consigliabile utilizzare in modo selettivo le annotazioni per individuare le informazioni e utilizzare l'oggetto metadati per fornire più contesto che aiuta a risolvere i problemi della richiesta dopo che è stata individuata.

Configurazione delle regole di campionamento di X-Ray

Bypersonalizzazione delle regole di campionamentoè possibile controllare la quantità di dati da registrare e modificare il comportamento di campionamento senza dover modificare o ridistribuire il

codice. Le regole di campionamento indicano all'SDK X-Ray il numero di richieste da registrare per una serie di criteri. Per impostazione predefinita, l'SDK X-Ray registrala 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 percentuale di richieste aggiuntive oltre la dimensione del serbatoio.

È necessario rivedere e aggiornare la configurazione predefinita per determinare un valore appropriato per il tuo account. Le richieste possono variare in base agli ambienti di sviluppo, test, test delle prestazioni e produzione. Potresti avere applicazioni che richiedono regole di campionamento personalizzate in base alla quantità di traffico ricevuta o al loro livello di criticità. Dovresti iniziare con una baseline e rivalutare regolarmente se la baseline soddisfa i tuoi requisiti.

Dashboard e visualizzazioni con CloudWatch

I dashboard consentono di concentrarsi rapidamente sulle aree di interesse per applicazioni e carichi di lavoro. CloudWatch fornisce dashboard automatici e puoi anche creare facilmente dashboard che utilizzano CloudWatch Parametri di CloudWatch i dashboard forniscono più informazioni rispetto alla visualizzazione isolata delle metriche perché consentono di correlare più metriche e identificare le tendenze. Ad esempio, un dashboard che include ordini ricevuti, memoria, utilizzo della CPU e connessioni al database può aiutarti a correlare le modifiche apportate alle metriche del carico di lavoro su piùAWSrisorse mentre il conteggio degli ordini aumenta o diminuisce.

È necessario creare dashboard a livello di account e applicazione per monitorare carichi di lavoro e applicazioni. Puoi iniziare utilizzando CloudWatch dashboard automatici, che sonoAWSdashboard a livello di servizio preconfigurati con metriche specifiche del servizio. I dashboard di assistenza automatici visualizzano tutto lo standard CloudWatch parametri per il servizio. I dashboard automatici illustrano tutte le risorse utilizzate per ogni metrica di servizio e ti aiutano a identificare rapidamente le risorse outlier nel tuo account. Ciò può aiutarti a identificare le risorse con un utilizzo elevato e basso, che può aiutarti a ottimizzare i costi.

Creazione di dashboard cross-service

È possibile creare dashboard cross-service visualizzando la dashboard automatica a livello di servizio per unAWSservizio e utilizzo delAggiungi a pannello di controlloopzione dalOperazionimenu. È quindi possibile aggiungere metriche da altri dashboard automatici alla nuova dashboard e rimuovere le metriche per restringere lo stato attivo del dashboard. È inoltre necessario aggiungere metriche personalizzate per tenere traccia delle osservazioni chiave (ad esempio, ordini ricevuti o transazioni al secondo). La creazione di un dashboard cross-service personalizzato 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 coprono le metriche chiave e visualizzino tutti i carichi di lavoro in un account.

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

Creazione di dashboard specifici per applicazioni o carichi di lavoro

Si consiglia 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. I

dashboard specifici per applicazioni e carichi di lavoro si concentrano sulle metriche personalizzate dell'applicazione o del carico di lavoro e importantiAWSmetriche delle risorse che influenzano le loro prestazioni.

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

Creazione di dashboard su più account o su più regioni

AWSle 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 di modificare le regioni per visualizzare metriche, dashboard e allarmi per carichi di lavoro e applicazioni tra regioni. Se separi le applicazioni e i carichi di lavoro in più account, potrebbe essere necessario eseguire nuovamente l'autenticazione e l'accesso a ciascun account. Tuttavia, CloudWatch supporta la visualizzazione di dati tra account e più regioni da un singolo account, il che significa che è possibile visualizzare metriche, allarmi, dashboard e widget di registro in un unico account e regione. Questo è molto utile se si dispone di un account di registrazione e monitoraggio centralizzato.

I proprietari di account e i proprietari del team di applicazioni devono creare dashboard per applicazioni specifiche per account e diverse regioni per monitorare efficacemente le metriche chiave in una posizione centralizzata. I dashboard di CloudWatch supportano automaticamente i widget multiregione, il che significa che è possibile creare un dashboard che include metriche da più regioni senza ulteriori configurazioni.

Un'eccezione importante è la CloudWatch Widget Logs Insights perché 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 la regione dai tuoi registri utilizzando i filtri delle metriche e queste metriche possono essere visualizzate in un dashboard tra regioni. È quindi possibile passare alla regione specifica quando è necessario analizzare ulteriormente tali registri.

I team operativi dovrebbero creare un dashboard centralizzato che monitora importanti metriche cross-account e cross-region. Ad esempio, è possibile creare un dashboard tra account che include l'utilizzo aggregato della CPU in ogni account e regione. È possibile utilizzare anchematematica delleper aggregare e controllare i dati tra molteplici account e regioni.

Utilizzo della matematica metrica per ottimizzare l'osservabilità e allarmante

È possibile utilizzare la matematica delle metriche per calcolare le metriche in formati ed espressioni rilevanti per i carichi di lavoro. Le metriche calcolate possono essere salvate e visualizzate su una dashboard a scopo di tracciamento. Ad esempio, le metriche standard di volume Amazon EBS forniscono il numero di letture (`VolumeReadOps`) e scrivi (`VolumeWriteOps`) operazioni eseguite in un determinato periodo.

Tuttavia,AWSfornisce linee guida sulle prestazioni del volume Amazon EBS in IOPS. Puoi disegnare e calcolare gli IOPS per il tuo volume Amazon EBS in matematica metrica aggiungendo il`VolumeReadOps`e`VolumeWriteOps` poi dividendo per il periodo scelto per queste metriche.

In questo esempio, riassumiamo gli IOPS nel periodo e quindi dividiamo per la lunghezza del periodo per ottenere l'IOPS. È quindi possibile impostare un allarme contro questa espressione matematica della metrica per avvisarti quando l'IOPS del volume si avvicina alla capacità massima per il tipo di volume. Per ulteriori informazioni ed esempi sull'utilizzo della matematica dei parametri per monitorare i file system Amazon Elastic File System (Amazon EFS) con CloudWatch metriche, vediAmazon CloudWatch metric math semplifica il monitoraggio quasi in tempo reale dei file system Amazon EFS e altro ancorasulAWSBlog.

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

CloudWatch Container Insights crea dashboard dinamici e automatici per i carichi di lavoro dei container in esecuzione su Amazon ECS e Amazon EKS. È consigliabile abilitare Container Insights per avere l'osservabilità di CPU, memoria, disco, rete e informazioni diagnostiche, come i guasti di riavvio del contenitore. Container Insights genera dashboard dinamici che è possibile filtrare rapidamente a livello di cluster, istanza contenitore o nodo, servizio, attività, pod e singoli contenitori. Container Insightsè configurato a livello di cluster e nodo o contenitorea seconda delAWSservizio.

Simile a Container Insights, CloudWatch Lambda Insights crea dashboard dinamici e automatici per le tue funzioni Lambda. Questa soluzione raccoglie, aggrega e riassume i parametri a livello di sistema, tra cui il tempo della CPU, la memoria, l'utilizzo del disco e della rete. Vengono inoltre raccolte, aggregate e riepilogate informazioni diagnostiche quali avvii a freddo e arresti del worker

Lambda per aiutare a isolare e risolvere rapidamente i problemi con le funzioni Lambda. Lambda è abilitato a livello di funzione e non richiede alcun agente.

Container Insights e Lambda Insights consentono inoltre di passare rapidamente ai log delle applicazioni o delle prestazioni, alle tracce dei X-Ray e a una mappa del servizio per visualizzare i carichi di lavoro dei container. Entrambi usano il CloudWatch formato dei parametri incorporati da acquisire CloudWatch log delle prestazioni e dei parametri.

È possibile creare una condivisione CloudWatch dashboard per il tuo carico di lavoro che utilizza le metriche acquisite da Container Insights e Lambda Insights. È possibile eseguire questa operazione filtrando e visualizzando il pannello di controllo automatico tramite CloudWatch Container Insights e quindi scegliere ilAggiungi a Dashboardopzione che consente di aggiungere le metriche visualizzate a una dashboard di CloudWatch standard. È quindi possibile rimuovere o personalizzare le metriche e aggiungere altre metriche per rappresentare correttamente il carico di lavoro.

Integrazione con CloudWatch conAWSservizi

AWSfornisce molti servizi che includono opzioni di configurazione aggiuntive per la registrazione e le metriche. Questi servizi spesso consentono di configurare CloudWatch Registri per l'output del log e CloudWatch metriche per l'output delle metriche. L'infrastruttura sottostante utilizzata per fornire questi servizi è gestita daAWSeè inaccessibile, ma è possibile utilizzare le opzioni di registrazione e metrica per i servizi sottoposti a provisioning per ottenere ulteriori informazioni e risolvere i problemi. Ad esempio, è possibile pubblicareRegistrazione di flusso VPC in CloudWatch, oppure puoi anche[configurare le istanze Amazon Relational Database Service (Amazon RDS) per pubblicare log in CloudWatch].

La maggior parteAWSi servizi registrano le chiamate API con[integrazione di adAWS CloudTrail]. CloudTrail anche[supporta l'integrazione con . CloudWatch Log]e questo significa che è possibile cercare e analizzare l'attività inAWSServizi . Puoi anche usare Amazon CloudWatch Eventi o Amazon EventBridge per creare e configurare automazione e notifiche con CloudWatch Regole eventi eventi per azioni specifiche eseguite inAWSServizi . Alcuni servizi[integrazione diretta di]con CloudWatch Eventi ed EventBridge. Puoi anche usare[creare eventi distribuiti tramite CloudTrail].

Amazon Managed Grafana per dashboard e visualizzazione

Amazon Managed Grafanapuò essere usato per osservare e visualizzare il tuoAWScarichi di lavoro. Amazon Managed Grafana ti aiuta a visualizzare e analizzare i tuoi dati operativi su larga scala. Grafanaè 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 di carichi di lavoro esistenti e desideri estendere la copertura aAWScarichi di lavoro. Puoi usare Amazon Managed Grafana con CloudWatch daaggiungendolo come origine dati, il che significa che è possibile creare visualizzazioni utilizzando CloudWatchParametri di Amazon Amazon Amazon GrafanaAWS Organizationse puoi centralizzare i dashboard usando CloudWatch Parametri da più account e regioni.

La tabella seguente fornisce i vantaggi e le considerazioni per l'utilizzo di Amazon Managed Grafana invece di CloudWatch per il pannello di controllo. 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 origini 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, tra cui CloudWatch Parametri di Amazon Managed Grafana include una serie di origini dati integrate che si estendonoAWSservizi, software open source e software COTS. Per ulteriori informazioni, consultaOrigine dati integratinella documenta zione di Amazon Managed Grafana. Puoi anche aggiungere il supporto per più origini dati aggiornando il tuo spazio di lavoro aGrafana. Grafanaplugin di origine datiche consenton o di comunicare con diversi sistemi esterni. CloudWatchi pannelli di controllo richiedon o un CloudWatch Parametro o CloudWatch Query di Logs Insights per i dati da visualizz are, visualizzare su un CloudWatch Pannello di controllo.

Gestisci l'accesso alla tua soluzione di dashboard separatamente dal tuoAWSaccesso ad account	Amazon Managed Grafana richiede l'utilizz o diAWS IAM Identity Center(IAM Identity Center) eAWS Organizationsper autenticazione e autorizzazione. Ciò consente di autenticare gli utenti su Grafana utilizzando la federazio ne delle identità che potresti già utilizzare con IAM Identity Center oAWS Organizations. Tuttavia, se non utilizzi IAM Identity Center oAWS Organizations, quindi viene impostato 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 oAWS Organizations.
Acquisisci e accedi ai dati su più account e aree geografiche conAWS Organizationsinteg razione	Amazon Amazon Amazon GrafanaAWS Organizationsper consentirti di leggere dati daAWSfonti come CloudWatch e Amazon e Amazon OpenSearch Servizio su tutti i tuoi account. In questo modo è possibile creare dashboard che visualizzano visualizzazioni utilizzando i dati di tutti i tuoi account. Per abilitare automaticamente l'accesso ai datiAWS Organizations, devi configurare il tuo spazio di lavoro Amazon GrafanaAWS Organizat ionsgestione dell'account. Questo non è consigliato in base aAWS Organizationsbest practice per l'account di gestione dell'acco unt. Al contrario, CloudWatch anchesupporta i pannelli di controllo su più account tra più regioni per CloudWatch metriche.

Utilizza widget di visualizzazione avanzati e definizioni di Grafana disponibili nella comunità open source	Grafana fornisce una vasta raccolta di visualizzazioni che è possibile utilizzare durante la creazione di dashboard. C'è anche una vasta libreria di dashboard forniti dalla comunità che puoi modificare e riutilizzare in base alle tue esigenze.
Utilizzare dashboard con implementazioni Grafana nuove ed esistenti	Se utilizzi già Grafana, puoi importare ed esportare dashboard dalle tue distribuzioni Grafana e personalizzarli per l'utilizzo 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 origini dati	Amazon Managed Grafana consente di creare più aree di lavoro Grafana che dispongono di un proprio set di origini dati, utenti e policy configurati. In questo modo è possibile soddisfare i requisiti dei casi d'uso più avanzati e le configurazioni di sicurezza avanzate. Le funzionalità avanzate potrebbero richiedere ai tuoi team di accrescere la loro esperienza con Grafana se non hanno già queste competenze.

Progettazione e implementazione di registrazioni e monitoraggio con CloudWatch DOMANDE FREQUENTI

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

Dove devo conservare il mio CloudWatch file di configurazione?

La CloudWatch agent per Amazon EC2 può applicare più file di configurazione archiviati nel CloudWatch directory di configurazione. Idealmente, è necessario memorizzare la configurazione di CloudWatch come un set di file perché è possibile controllare la versione e riutilizzarli in più account e ambienti. Per ulteriori informazioni, consulta la sezioneGestione delle configurazioni CloudWatchsezione di questa guida. In alternativa, è possibile archiviare i file di configurazione in un repository su GitHub e automatizza il recupero dei file di configurazione quando viene eseguito il provisioning di una nuova istanza EC2.

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

Integra il tuo sistema di gestione dei servizi con un argomento Amazon Simple Notification Service (Amazon SNS) e configura CloudWatch allarme per notificare l'argomento SNS quando viene generato un allarme. Il sistema integrato riceve il messaggio SNS e può creare un ticket utilizzando le API o gli SDK dei sistemi di gestione dei servizi.

Come si usa CloudWatch per catturare i file di registro nei miei contenitori?

Le attività 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 di applicazioni containerizzate consiste nel far in modo che i container inviino il loro output a STDOUT e STDERR. Questo è anche trattato nelManifesto app a dodici fattori.

Tuttavia, se si desidera inviare file di registro specifici a CloudWatch quindi puoi montare un volume nel tuo pod Amazon EKS o nella definizione di attività Amazon ECS in cui l'applicazione scriverà

i suoi file di lotto e utilizzerà un contenitore sidecar per Fluentd o Fluent Bit per inviare i log a CloudWatch. Dovresti considerare il collegamento simbolico di un file di registro specifico nel tuo contenitore a`/dev/stdout`e`/dev/stderr`. Per ulteriori informazioni, consultaVisualizza i registri per un contenitore o un servizionella documentazione Docker.

Come posso monitorare i problemi di salute perAWSservices?

Puoi utilizzare il pluginAWS Health Dashboardper monitorareAWSeventi sull'integrità di Puoi anche fare riferimento aaws-health tools GitHub repository per soluzioni di automazione campione relative aAWSeventi sull'integrità di

Come posso creare un personalizzato CloudWatch metrica quando non esiste alcun supporto agente?

Puoi utilizzare il formato metrico incorporato per inserire parametri in CloudWatch. È possibile utilizzare ancheAWSSDK (ad esempio,put_metric_data),AWS CLI(ad esempio,put-metric-data), oppureAWSAPI (ad esempio,PutMetricData) per creare parametri personalizzati. Dovresti considerare come qualsiasi logica personalizzata verrà mantenuta a lungo termine. Un approccio sarebbe quello di utilizzare Lambda con supporto integrato per il formato metrico integrato per creare le tue metriche, insieme a CloudWatch Eventiregola di pianificazioneper stabilire il periodo per la metrica.

Come integro i miei strumenti di registrazione e monitoraggio esistenti conAWS?

È necessario fare riferimento alle indicazioni fornite dal software o dal fornitore di servizi per l'integrazione conAWS. 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. È possibile utilizzare anche ilAWSSDK e CloudWatch Registra i filtri di abbonamento con Lambda e Kinesis Data Streams per creare processori di log e spedizionieri personalizzati. Infine, dovresti anche considerare come integrare il software se utilizzi più account e regioni.

Risorse

Introduzione

- AWSWell-Architected

Risultati di business mirati

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

Pianificazione CloudWatch della distribuzione

- Concetti e terminologia AWS Organizations
- AWS Systems ManagerConfigurazione rapida
- Raccolta di parametri e log da istanze Amazon EC2 e da server on-premise con l' CloudWatch agente
- cloudwatch-config-s3 secchi.yaml
- Creazione del file di configurazione dell' CloudWatch agente tramite la procedura guidata
- Enterprise DevOps: perché dovresti eseguire ciò che costruisci
- Esportazione di dati di registro in Amazon S3
- Controllo granulare degli accessi nel OpenSearch servizio di Amazon
- Quote di Lambda
- Creazione o modifica manuale del file di configurazione CloudWatch dell'agente
- Elaborazione in tempo reale dei dati di registro con le sottoscrizioni
- Strumenti su cui costruireAWS

Configurazione dell' CloudWatch agente per istanze EC2 e server on-premise

- Dimensioni dei parametri Amazon EC2

- Istanze di prestazioni espandibili
- CloudWatch Insieme di parametri predefiniti dell'agente
- Raccolta di parametri dei processi con il plug-in procstat
- Configurazione dell' CloudWatch agente per procstat
- Abilitazione o disabilitazione del monitoraggio dettagliato per le istanze
- Importazione di registri ad alta cardinalità e generazione di parametri con CloudWatch Metric Format
- Utilizzo di gruppi di log e flussi di log
- Elencare i CloudWatch parametri di disponibili per le istanze
- PutLogEvents
- Recupero dei parametri personalizzati con collectd
- Recupero dei parametri personalizzati con StatsD

CloudWatch approcci all'installazione degli agenti per Amazon EC2 e server locali

- Creare un ruolo di servizio IAM per un ambiente ibrido
- Creazione di un'attivazione di un'istanza gestita per un ambiente ibrido
- Creazione di ruoli e utenti IAM da usare con l' CloudWatch agente
- Download e configurazione dell' CloudWatch agente tramite la riga di comando
- Come posso configurare i server locali che utilizzano l'agente Systems Manager e l' CloudWatchagente unificato per utilizzare solo credenziali temporanee?
- Prerequisiti per le operazioni dei set di stack
- Utilizzo delle istanze spot

Logging e monitoraggio su Amazon ECS

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

- Agente del container di Amazon ECS
- Tipi di avvio di Amazon ECS
- Implementazione dell' CloudWatch agente per raccogliere parametri a livello di istanza EC2 su Amazon ECS
- ecs_cluster_with_cloudwatch_linux.yaml
- ecs_cw_emf_esempio
- ecs_firelense_emf_esempio
- ecs-task-nginx-firelense.json
- Recupero dei metadati AMI ottimizzati per Amazon ECS
- Utilizzo del driver di log awslogs
- Utilizzo di librerie client per generare log in Embedded Metric Format

Logging 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 dei parametri di Container Insights Prometheus
- Metriche del piano di controllo con Prometheus
- Implementazione di Kubernetes Dashboard (Interfaccia utente Web)
- 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 parametri Prometheus
- Installazione di Kubernetes Metrics Server
- kubernetes /dashboard
- Scalatore automatico Kubernetes Horizontal Pod
- Componenti Kubernetes Control Plane

- Pod Kubernetes
- Supporto modello di avvio
- Gruppi di nodi gestiti
- Comportamento di aggiornamento del nodo gestito
- server di metriche
- Monitoraggio di Amazon EKS su Fargate utilizzando Prometheus e Grafana
- prometheus_jmx
- prometeo/jmx_exporter
- Scraping di ulteriori origini Prometheus e importazione di tali parametri
- Nodi autogestito
- Invia registri ai CloudWatch registri
- Configurazione di FluentD come DaemonSet a per inviare log a CloudWatch Logs
- Configurazione del carico di lavoro di esempio Java/JMX su Amazon EKS e Kubernetes
- Esercitazione per l'aggiunta di una nuova destinazione di scraping Prometheus: parametri del server API Prometheus
- Scaler automatico Vertical Pod

Registrazione e metriche perAWS Lambda

- Errori di chiamata Lambda
- logging — Funzione di registrazione per Python
- Utilizzo di librerie client per generare log in Embedded Metric Format
- Utilizzo dei parametri delle funzioni Lambda

Ricerca e analisi dei log in CloudWatch

- La famiglia Beats
- Logstash elastico
- Pila elastica
- Streaming dei dati dei CloudWatch log su Amazon OpenSearch Service

Opzioni allarmanti con CloudWatch

- amazon-cloudwatch-auto-alarms
- AWSConnettore di gestione dei servizi per Jira Service Management
- AWSService Management Connector per ServiceNow

Monitoraggio della disponibilità di applicazioni e servizi

- Configurazione di un failover DNS

Tracciamento delle applicazioni conAWS X-Ray

- Rete di processi di 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 a X-Ray

Dashboard e visualizzazioni con CloudWatch

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

CloudWatch integrazione conAWS i servizi

- Servizi e integrazioni AWS CloudTrail supportati
- CloudWatch Eventi ed esempi di eventi dai servizi supportati
- Eventi erogati tramite CloudTrail

- Monitoraggio dei file di CloudTrail registro con CloudWatch Logs
- Pubblicazione di log del motore di database in CloudWatch Logs
- Pubblicazione di log di flusso in CloudWatch Loggs

Amazon Managed Grafana per dashboard e visualizzazione

- Best practice per l'account di gestione inAWS Organizations
- Fonti di dati integrate per Amazon Managed Grafana
- Dashboard tra account e regioni in CloudWatch
- Plugin Grafana

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti apportate a questa guida. Se desideri ricevere una notifica sugli aggiornamenti future, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Informazioni di registrazione aggiornate	È stata aggiornata la sezione sulla registrazione perAWS Lambda.	17 aprile 2023
Informazioni di configurazione aggiornate	È stata aggiornata e rinominat a la sezione relativa alla creazione e all'archiviazione CloudWatch delle configura zioni.	9 febbraio 2023
Informazioni aggiornate sulle metriche	Sono state aggiornate le informazioni sulle metriche personalizzate dell'appl icazione nella sezione Metriche per Amazon ECS.	31 gennaio 2023
Avvisi di anteprima rimossi	Amazon Managed Grafana è disponibile a livello generale.	25 maggio 2022
Sezione rimossa	CloudWatch SDK Metrics non è più supportato.	7 gennaio 2022
Pubblicazione iniziale	—	30 aprile 2021

Glossario del Prontuario AWS

I seguenti termini sono comunemente utilizzati in strategie, guide e pattern forniti dal Prontuario AWS. 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: esegui la migrazione del database Oracle on-premise ad Amazon Aurora edizione compatibile con 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: esegui la migrazione del database Oracle on-premise ad Amazon Relational Database Service (Amazon RDS) per Oracle nel 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: esegui la migrazione del 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: esegui la migrazione del tuo database Oracle on-premise su Oracle su un'istanza EC2 nel 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. Questo scenario di migrazione è specifico di VMware Cloud su AWS, che supporta la compatibilità delle macchine virtuali (VM) e la portabilità del carico di lavoro tra l'ambiente on-premise e AWS. È possibile utilizzare le tecnologie VMware Cloud Foundation dai data center on-premise durante la migrazione dell'infrastruttura a VMware Cloud su AWS. Esempio: trasferisci l'hypervisor che ospita il database Oracle su VMware Cloud su AWS.
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a

un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.

- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione aggregata

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, consulta ABAC per AWS nella documentazione di 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

Posizione separata all'interno di una Regione AWS isolata dagli errori che si verificano in altre zone di disponibilità che offre connettività di rete non costosa e a bassa latenza ad altre zone di disponibilità nella stessa regione.

Framework per l'adozione del cloud AWS (AWS CAF)

Un framework di linee guida e buone pratiche di 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: azienda, 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. Per questa prospettiva, AWS CAF fornisce linee guida per lo sviluppo del personale, la formazione e le comunicazioni per aiutare l'organizzazione nell'adozione efficace del cloud. Per ulteriori informazioni, consulta il sito web di AWS CAF e il white paper AWS CAF.

AWS Workload Qualification Framework (AWS WQF)

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

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.

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, vedere About branch (GitHub documentazione).

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-ArchitectedAWS.

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 AWSCloud Adoption Framework.

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 in locale, prima che vengano ricevuti dal Servizio AWS di destinazione.

centro di eccellenza del cloud (CCoE)

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

cloud computing

La tecnologia cloud generalmente utilizzata per l'archiviazione remota di dati e la gestione dei dispositivi IoT. Il cloud computing è comunemente 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 il cloud AWS:

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

Queste fasi sono state definite da Stephen Orban nel post del blog The Journey Toward Cloud-First & the Stages of Adoption sul blog AWS Cloud Enterprise Strategy. Per informazioni su come si relazionano alla strategia di migrazione AWS, consulta la guida di 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 oAWS CodeCommit. Ogni versione del codice è denominata ramo. In una struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola pipeline CI/CD può utilizzare più repository.

cache fredda

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

dati freddi

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

visione artificiale

Un campo dell'intelligenza artificiale utilizzato dalle macchine per identificare persone, luoghi e cose nelle immagini con una precisione pari o superiore ai livelli umani. Spesso costruito con modelli di deep learning, automatizza l'estrazione, l'analisi, la classificazione e la comprensione di informazioni utili da una singola immagine o da una sequenza di immagini.

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 serie di regole di AWS Config e azioni correttive che puoi riunire per personalizzare i controlli di conformità e sicurezza. Puoi distribuire un pacchetto di conformità come singola entità in un Account AWS e in una regione, o all'interno di un'organizzazione, utilizzando un modello YAML. Per ulteriori informazioni, consulta Pacchetti di conformità nella documentazione di AWS Config.

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

Il processo di automazione delle fasi di origine, creazione, test, gestione temporanea e produzione del processo di rilascio del software. Il processo CI/CD è comunemente descritto come una pipeline. CI/CD può aiutare ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le distribuzioni. Per ulteriori informazioni, consulta Vantaggi della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

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 Framework AWS Well-Architected. 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.

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'AWSambiente 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 adotti questa strategia in AWS, puoi aggiungere più controlli a diversi livelli della struttura AWS Organizations 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 membro di AWS 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 suAWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

edge computing

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

Un servizio che puoi ospitare in un cloud privato virtuale (VPC) da condividere con altri utenti. Puoi creare un servizio endpoint con AWS PrivateLink e concedere le autorizzazioni ad altri Account AWS o ai principali AWS Identity and Access Management (IAM). 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).

crittografia envelope

Il processo di crittografia di una chiave di crittografia con un'altra chiave di crittografia. Per ulteriori informazioni, consulta Crittografia a busta nella documentazione di AWS Key Management Service (AWS KMS).

ambiente

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

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

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

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione. Ad esempio le epiche di 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.

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

NelCloud AWS, un limite come una zona di disponibilitàRegione 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 AWSFault Isolation Boundaries.

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

G

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. AWS offre AWS SCT che aiuta con le conversioni dello schema.

alta disponibilità (HA)

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

modernizzazione storica

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

migrazione di database omogenea

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

dati caldi

Dati a cui si accede frequentemente, 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

Considera l'infrastruttura come codice.

Policy basata su identità

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

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 multi-account AWS, un VPC che accetta, ispeziona e instrada le connessioni di rete dall'esterno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

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

infrastruttura

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

infrastruttura come codice (IaC)

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

Internet delle cose industriale (IIoT)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione Machine learning.

ramo principale

Vedi filiale.

servizi gestiti

Servizi AWSper 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.

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 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.

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

Un programma AWS che offre consulenza, 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 negli 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 di destinazione, il gruppo di sicurezza e l'account 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: eseguire il rehosting della migrazione ad Amazon EC2 con AWS Application Migration Service.

Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione al 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 il login) è disponibile gratuitamente per tutti i consulenti AWS e i consulenti partner APN.

valutazione della preparazione alla migrazione (MRA)

Il processo di acquisizione di informazioni sullo stato di idoneità 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 AWS CAF. 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 eseguire la migrazione di un carico di lavoro verso il 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.

MAPPA

Vedi Migration Portfolio Assessment.

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, consulta la sezione Strategia per modernizzare le applicazioni nel 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, consulta la sezione Valutazione della preparazione alla modernizzazione per le applicazioni nel 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.

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.

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.

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 trail creato da AWS CloudTrail che registra tutti gli eventi per tutti gli Account AWS in un'organizzazione di 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, vedere Creazione di un percorso per un'organizzazione nella documentazione. CloudTrail

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 migrazione AWS, 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 tutte le Regioni AWS, crittografia lato server con AWS KMS (SSE-KMS) e richieste `PUT` e `DELETE` dinamiche al bucket S3.

identità di accesso origine (OAI)

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

O

Vedi la revisione della prontezza operativa.

VPC in uscita (egress)

In un'architettura multi-account AWS, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

Privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

Ambiente di produzione

Vedi ambiente.

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.

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

Il periodo di tempo massimo accettabile dall'ultimo punto di ripristino dei dati. Ciò determina quella che viene considerata una perdita di dati accettabile tra l'ultimo punto di ripristino e l'interruzione del servizio.

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Regione

Una raccolta di risorse AWS in un'area geografica. Ogni Regione AWS è isolata e indipendente dalle altre per fornire tolleranza agli errori, stabilità e resilienza. Per ulteriori informazioni, consulta Gestione delle Regioni AWS nei Riferimenti generali di AWS.

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.

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

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

S

SAML 2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità consente l'autenticazione unica (SSO) federata, grazie alla quale gli utenti possono accedere alla AWS Management Console o eseguire chiamate alle operazioni delle API AWS. In questo modo non è necessario creare un utente IAM per tutti gli utenti nell'organizzazione. Per ulteriori informazioni sulla federazione basata su SAML 2.0, consulta Informazioni sulla federazione basata su SAML 2.0 nella documentazione di IAM.

SCP

Vedi la politica di controllo del servizio.

Secret

InAWS Secrets Manager, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, consulta Secret nella documentazione di Secrets Manager.

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

Crittografia dei dati a destinazione, da parte del Servizio AWS che li riceve.

Policy di controllo dei servizi (SCP)

Una policy che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in AWS Organizations. Le SCP definiscono i guardrail o fissano i limiti alle azioni che un amministratore può delegare a utenti o ruoli. Puoi utilizzare le SCP come elenchi

consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta Policy di sicurezza dei servizi nella documentazione di AWS Organizations.

endpoint del servizio

L'URL del punto di accesso 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 con AWS per la sicurezza e la conformità del cloud. AWS è responsabile della sicurezza del cloud, mentre l'utente è 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.

crittografia simmetrica

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

test sintetici

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

T

tags

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

variabile di destinazione

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

elenco di attività

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

Ambiente di test

Vedi ambiente.

training

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

Transit Gateway

Un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti on-premise. Per ulteriori informazioni, consulta Che cos'è un Transit Gateway? nella documentazione di AWS Transit Gateway.

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

La concessione di autorizzazioni a un servizio specificato dall'utente per eseguire attività all'interno dell'organizzazione in AWS Organizations e nei relativi 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 di AWS Organizations con altri servizi AWS nella documentazione di AWS Organizations.

regolazione

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

team da due pizze

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

U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

Una funzione SQL che esegue un calcolo su un gruppo di righe che si riferiscono in qualche modo al record corrente. Le funzioni della finestra sono utili per l'elaborazione di attività, come il calcolo

di una media mobile o l'accesso al valore delle righe in base alla posizione relativa della riga corrente.

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

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

vulnerabilità zero-day

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

applicazione zombie

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

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