Raggiungimento della maturità di Essential Eight il AWS

# AWS Guida prescrittiva

# AWS Guida prescrittiva: Raggiungimento della maturità di Essential Eight il AWS

# Table of Contents

# Raggiungere la maturità di Essential Eight in materia di AWS: sicurezza e conformità per le organizzazioni australiane

Amazon Web Services (collaboratori)

Novembre 2024 (cronologia dei documenti)

L'Australian Signals Directorate (ASD) ha creato e dato priorità a strategie per aiutare le organizzazioni a mitigare i rischi delle minacce alla sicurezza informatica. Otto di queste strategie sono state scelte per formare il framework Essential Eight. Molte organizzazioni del settore pubblico e privato in Australia devono raggiungere la maturità nell'ambito del quadro Essential Eight.

L'Australian Cyber Security Centre (ACSC) ha creato il framework Essential Eight per aiutare a proteggere le reti Microsoft basate su Internet. Tuttavia, molte organizzazioni devono raggiungere la maturità di Essential Eight per tutti i loro ambienti, sia on-premise che nel cloud.

Il framework Essential Eight include anche un modello di maturità progettato per aiutare le organizzazioni a implementare il framework attraverso un'iterazione progressiva. Il modello delinea i livelli di maturità da zero a tre. Il terzo livello di maturità rappresenta la resilienza contro tattiche avanzate di sicurezza informatica e attacchi altamente mirati. Questa guida fornisce una guida specifica e ponderata per aiutarvi a raggiungere il terzo livello di maturità di Essential Eight. AWS

# Sicurezza e conformità per le organizzazioni australiane

Molte organizzazioni in Australia lo utilizzano Cloud AWS per archiviare dati riservati, elaborare transazioni sensibili e creare servizi critici.

Sebbene questa guida spieghi come adattare il framework Essential Eight per il cloud, fornisce AWS anche le seguenti certificazioni e modelli per aiutarti a soddisfare i requisiti di sicurezza e conformità della tua organizzazione:

- Programma di valutazione registrati per la sicurezza delle informazioni
- Framework di certificazione dell'hosting
- AWS modello di responsabilità condivisa
- AWS Well-Architected Framework

## Programma di valutazione registrati per la sicurezza delle informazioni

Servizi AWS sono stati valutati nell'ambito dell'Australian Cyber Security Centre (ACSC) Information Security Registered Assessors Program (IRAP) a livello PROTECTED. Un valutatore indipendente certificato IRAP dall'Australian Signals Directorate (ASD) ha completato la valutazione IRAP di. AWS Questa valutazione garantisce che, per quanto riguarda i AWS prodotti e i servizi, i controlli applicabili siano implementati per i carichi di lavoro di livello PROTECTED.

Il pacchetto AWS IRAP PROTECTED è disponibile tramite. AWS Artifact Il rapporto IRAP è stato sviluppato utilizzando le linee guida sulla sicurezza di ACSC Cloud (sito web ACSC). Per un elenco completo di Servizi AWS ciò che rientra nell'ambito, vedere Servizi AWS in scope: IRAP.

## Framework di certificazione dell'hosting

L'Australian Hosting Certification Framework è stato sviluppato per supportare la gestione sicura dei sistemi e dei dati governativi. Questo framework ha lo scopo di aiutare le organizzazioni a mitigare i rischi della catena di approvvigionamento e della proprietà dei data center. AWS ha ottenuto la certificazione a livello Certified Strategic. Questo aiuta le agenzie governative a continuare a innovare a un ritmo rapido, sapendo che AWS soddisfa i requisiti governativi.

# AWS modello di responsabilità condivisa

Il modello di responsabilitàAWS condivisa definisce il modo in cui condividi la responsabilità AWS per la sicurezza e la conformità nel cloud. AWS protegge l'infrastruttura che gestisce tutti i servizi offerti nel e l' Cloud AWS utente è responsabile della protezione dell'uso di tali servizi, come dati e applicazioni.

Questo modello condiviso può contribuire ad alleggerire la conformità e l'onere operativo perché AWS gestisce, gestisce e controlla molti componenti, dal sistema operativo host e dal livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui opera il servizio. L'utente si assume la responsabilità della gestione del sistema operativo guest (inclusi gli aggiornamenti e le patch di sicurezza) e degli altri software applicativi associati. L'utente si assume inoltre la responsabilità della configurazione del firewall del gruppo di sicurezza che AWS fornisce.

È fondamentale comprendere il modello di responsabilità AWS condivisa quando ci si avvicina alla maturità di Essential Eight. AWS Le vostre responsabilità variano a seconda dei servizi utilizzati, dell'integrazione di tali servizi nell'ambiente IT e delle leggi e dei regolamenti applicabili.

# AWS Well-Architected Framework

AWS Well-Architected aiuta gli architetti del cloud a creare un'infrastruttura sicura, ad alte prestazioni, resiliente ed efficiente per una varietà di applicazioni e carichi di lavoro. AWS Well-Architected Framework fornisce le migliori pratiche architettoniche che consentono di progettare, creare e utilizzare sistemi su. AWS Questo framework si basa su sei pilastri: eccellenza operativa, sicurezza, affidabilità, efficienza delle prestazioni, ottimizzazione dei costi e sostenibilità.

AWS fornisce anche un servizio per la revisione dei carichi di lavoro. Ti AWS Well-Architected Toolaiuta a rivedere e valutare la tua architettura utilizzando il AWS Well-Architected Framework. Fornisce consigli per rendere i carichi di lavoro più affidabili, sicuri, efficienti ed economici.

# Reinterpretazione delle otto strategie essenziali per il cloud

Di seguito sono riportate le strategie di mitigazione originali di Essential Eight progettate per reti connesse Microsoft a Internet basate su:

- Controllo delle applicazioni
- Applicazioni di patch
- Configura le impostazioni delle Microsoft Office macro
- Rafforzamento delle applicazioni utente
- Limita i privilegi amministrativi
- Patch i sistemi operativi
- Autenticazione a più fattori
- Backup regolari

È importante ribadire che il framework Essential Eight non è progettato per ambienti cloud. Tuttavia, i principi di base sono applicabili e vi è una sovrapposizione tra le strategie Essential Eight e le migliori pratiche del AWS Well-Architected Framework.

Diversi approcci nativi del cloud possono migliorare la sicurezza e ridurre drasticamente il carico di conformità. Negli ambienti locali, l'utente è responsabile di tutti gli aspetti della sicurezza e non esistono controlli ereditati. Quando esegue carichi di lavoro nel cloud, AWS è responsabile della protezione dell'infrastruttura che gestisce i nostri servizi. Puoi anche ridurre il carico di conformità utilizzando l'automazione e i servizi gestiti. I servizi gestiti, noti anche come servizi astratti, consentono Servizi AWS AWS di gestire il livello di infrastruttura, il sistema operativo e le piattaforme e di accedere 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. Per ulteriori informazioni, consulta la Tema 1: Utilizzare i servizi gestiti sezione di questa guida.

Pertanto, è necessaria una certa reinterpretazione per rendere le strategie Essential Eight appropriate per i carichi di lavoro. AWSQuesta guida converte le strategie Essential Eight in temi. AWS

# Utilizzo dei temi

Questa guida è suddivisa in otto temi. Ogni strategia Essential Eight è mappata su uno o più dei seguenti temi e ogni tema è mappato su una o più best practice nel Well-Architected AWS Framework:

- Tema 1: Utilizzare i servizi gestiti
- Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure
- Tema 3: Gestisci l'infrastruttura mutabile con l'automazione
- Tema 4: Gestire le identità
- Tema 5: Stabilire un perimetro di dati
- Tema 6: Automatizza i backup
- Tema 7: Centralizzare la registrazione e il monitoraggio
- Tema 8: Implementazione di meccanismi per i processi manuali

Ogni tema include una panoramica dell'argomento, le best practice correlate di AWS Well-Architected Framework e istruzioni su come raggiungere la maturità di Essential Eight e monitorare la conformità. Le istruzioni forniscono passaggi manuali o aiutano a configurare le automazioni utilizzando le regole.AWS Config Le procedure manuali richiedono meccanismi per garantire che i risultati vengano risolti. Per ulteriori informazioni, vedereTema 8: Implementazione di meccanismi per i processi manuali. AWS Config le regole richiedono una supervisione o un'automazione simili per porre rimedio alle risorse non conformi. Seguendo le linee guida in linea con questi temi, puoi raggiungere la maturità di Essential Eight con un approccio che massimizza anche i vantaggi del cloud.

# Reinterpretazione delle strategie Essential Eight per il cloud

Poiché il framework Essential Eight non è progettato per ambienti cloud, è essenziale adottare un approccio nativo del cloud nell'affrontare i principi alla base di ciascuna strategia Essential Eight. L'approccio varia in base a due domande chiave.

## Quali servizi stai utilizzando?

AWS modello di responsabilità condivisaPossono contribuire ad alleggerire gli oneri operativi e di conformità. I servizi gestiti trasferiscono maggiori AWS responsabilità al mantenimento della disponibilità, delle prestazioni e dell'ottimizzazione della sicurezza del servizio distribuito. I servizi

gestiti eliminano inoltre l'onere operativo e amministrativo della manutenzione di un servizio, offrendo più tempo per concentrarsi sull'innovazione.

I servizi gestiti includono servizi serverless, come Amazon API Gateway e DynamoDB. AWS Lambda Un database su Amazon Relational Database Service (Amazon RDS) richiede meno responsabilità operative rispetto a un database su Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute Cloud (Amazon EC2).

Ad esempio, se stai adattando la strategia Essential Eight del sistema operativo Patch per il cloud, devi considerare quali servizi stai utilizzando e se sei responsabile dell'applicazione delle patch a tali risorse. AWS è responsabile dell'applicazione di patch a servizi completamente gestiti, come Lambda e DynamoDB. Per altri servizi, come Amazon RDS o Amazon Redshift, potrebbe essere necessario gestire le patch durante le finestre di manutenzione.

## Quale modello di distribuzione stai utilizzando?

La tua organizzazione utilizza un approccio all'infrastruttura mutevole o immutabile?

Il modello di infrastruttura mutabile aggiorna e modifica l'infrastruttura esistente per i carichi di lavoro di produzione. Questo era il metodo di implementazione standard prima del cloud, quando la sostituzione dell'infrastruttura dei server era così costosa e dispendiosa in termini di tempo che l'approccio più pratico consisteva nell'applicare le modifiche ai server già in produzione. Un esempio di approccio mutevole nel cloud è l'implementazione delle modifiche alle applicazioni direttamente sulle istanze EC2 in esecuzione, manualmente o utilizzando un servizio di distribuzione del software, come Run Command o.AWS Systems ManagerAWS CodeDeploy

Il modello di infrastruttura immutabile implementa una nuova infrastruttura per i carichi di lavoro di produzione anziché aggiornare, applicare patch o modificare l'infrastruttura esistente. Un esempio di approccio immutabile è la definizione di uno stack di applicazioni in or. AWS CloudFormationAWS Cloud Development Kit (AWS CDK) È possibile utilizzare questi servizi per distribuire uno stack di applicazioni tramite pipeline di integrazione e distribuzione continua (CI/CD). Questo approccio utilizza metodi di implementazione come rolling o blue/green. Per ulteriori informazioni su questo approccio, consulta la best practice Deploy using immutable infrastructure nel Well-Architected AWS Framework.

Ad esempio, se stai adattando la strategia Essential Eight del sistema operativo Patch per il cloud, devi considerare in che modo l'applicazione delle patch si applica al modello di implementazione. Per un'infrastruttura mutevole, è possibile applicare manualmente le patch alle risorse o migliorare l'efficienza operativa attraverso l'automazione. Se utilizzi un'infrastruttura immutabile, utilizzerai una

CI/CD pipeline per implementare una nuova infrastruttura con l'ultima versione del sistema operativo. In effetti, il termine patching è un termine improprio in questo modello perché l'infrastruttura verrebbe sostituita anziché patchata.

# Tema 1: Utilizzare i servizi gestiti

Otto strategie essenziali coperte

Applicate patch alle applicazioni, limitate i privilegi amministrativi, applicate le patch ai sistemi operativi

I servizi gestiti aiutano a ridurre gli obblighi di conformità consentendo di AWS gestire alcune attività di sicurezza, come l'applicazione di patch e la gestione delle vulnerabilità.

Come illustrato nella AWS modello di responsabilità condivisa sezione, condividete la responsabilità AWS per la sicurezza e la conformità del cloud. Ciò può ridurre l'onere operativo in quanto AWS gestisce, gestisce e controlla i componenti, dal sistema operativo host e dal livello di virtualizzazione alla sicurezza fisica delle strutture in cui opera il servizio.

Le tue responsabilità potrebbero includere la gestione delle finestre di manutenzione per i servizi gestiti, come Amazon Relational Database Service (Amazon RDS) o Amazon Redshift, e la scansione delle vulnerabilità AWS Lambda nel codice o nelle immagini dei container. Come per tutti i temi di questa guida, anche tu hai la responsabilità del monitoraggio e dei report di conformità. Puoi utilizzare Amazon Inspector per segnalare vulnerabilità su tutti i tuoi dispositivi. Account AWS Puoi utilizzare le regole AWS Config per assicurarti che i servizi, come Amazon RDS e Amazon Redshift, abbiano aggiornamenti minori e finestre di manutenzione abilitate.

Ad esempio, se esegui un'istanza Amazon EC2, le tue responsabilità includono quanto segue:

- Controllo delle applicazioni
- Applicazioni di applicazione di patch
- Limitazione dei privilegi amministrativi al piano di controllo di Amazon EC2 e al sistema operativo (OS)
- Applicazione di patch al sistema operativo
- Applicazione dell'autenticazione a più fattori (MFA) per accedere al piano di AWS controllo e al sistema operativo
- Backup dei dati e della configurazione

Se invece esegui una funzione Lambda, le tue responsabilità sono ridotte e includono quanto segue:

- Controllo delle applicazioni
- Conferma che le librerie sono up-to-date
- Limitazione dei privilegi amministrativi al piano di controllo Lambda
- Applicazione dell'MFA per accedere al piano di controllo AWS
- Backup del codice e della configurazione della funzione Lambda

# Best practice correlate nel AWS Well-Architected Framework

- SEC01- BP05 Ridurre l'ambito di gestione della sicurezza

# Implementazione di questo tema

## Abilita l'applicazione di patch

- Applica gli aggiornamenti di Amazon RDS
- Abilita gli aggiornamenti gestiti in AWS Elastic Beanstalk
- Sii consapevole delle finestre di manutenzione dei cluster Amazon Redshift

## Scansiona le vulnerabilità

- Scansiona le immagini dei container Amazon Elastic Container Registry (Amazon ECR) con Amazon Inspector
- Funzioni di scansione Lambda con Amazon Inspector

# Monitoraggio di questo tema

## Implementa controlli di governance

- Abilita il pacchetto di conformità Operational Best Practices for ACSC Essential 8 AWS Config

## Monitoraggio di Amazon Inspector

- Valuta la copertura a livello di account

- Gestisci più account

## Implementa le seguenti AWS Config regole

- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EKS_CLUSTER_SUPPORTED_VERSION

# Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure

Otto strategie essenziali coperte

Controllo delle applicazioni, applicazioni di patch, sistemi operativi di patch

Per un'infrastruttura immutabile, è necessario proteggere le pipeline di distribuzione per le modifiche al sistema. AWS L'illustre ingegnere Colm MacCárthaigh ha spiegato questo principio nella presentazione (video) di Zero-Privilege Operations: Running Services Without Access to Data alla conferenza re:Invent del 2022. YouTube AWS

Limitando l'accesso diretto alle risorse di configurazione, è possibile richiedere che tutte AWS le risorse vengano distribuite o modificate tramite pipeline approvate, protette e automatizzate. Di solito, si creano policy AWS Identity and Access Management (IAM) che consentono agli utenti di accedere solo all'account che ospita la pipeline di distribuzione. Puoi anche configurare le policy IAM che consentono l'accesso ininterrotto per un numero limitato di utenti. Per evitare modifiche manuali, puoi utilizzare i gruppi di sicurezza per bloccare l'accesso SSH e RDP (WindowsRemote Desktop Protocol) ai server. Session Manager, una funzionalità di AWS Systems Manager, può fornire l'accesso alle istanze senza la necessità di aprire le porte in ingresso o gestire gli host bastion.

Amazon Machine Images (AMI) e le immagini dei container devono essere create in modo sicuro e ripetibile. Per le istanze Amazon EC2, puoi utilizzare EC2 Image Builder per AMIs creare versioni con funzionalità di sicurezza integrate, come l'individuazione delle istanze, il controllo delle applicazioni e la registrazione. Per ulteriori informazioni sul controllo delle applicazioni, consulta Implementing Application Control sul sito Web ACSC. Puoi anche usare Image Builder per creare immagini di container e puoi usare Amazon Elastic Container Registry (Amazon ECR) Elastic Container Registry (Amazon ECR) per condividere tali immagini tra account. Un team di sicurezza centrale può approvare il processo automatizzato per la creazione di queste immagini AMIs e dei container in modo che qualsiasi AMI o immagine del contenitore risultante venga approvata per l'uso da parte dei team applicativi.

Le applicazioni devono essere definite in Infrastructure as Code (IaC), utilizzando servizi come AWS CloudFormationo. AWS Cloud Development Kit (AWS CDK) Gli strumenti di analisi del codice AWS CloudFormation Guard, come cfn-nag o cdk-nag, possono testare automaticamente il codice rispetto alle migliori pratiche di sicurezza nella pipeline approvata.

Allo stesso modoTema 1: Utilizzare i servizi gestiti, Amazon Inspector può segnalare le vulnerabilità in tutto il tuo. Account AWS I team centralizzati di cloud e sicurezza possono utilizzare queste informazioni per verificare che il team applicativo soddisfi i requisiti di sicurezza e conformità.

Per monitorare e generare report sulla conformità, esegui revisioni continue delle risorse e dei log IAM. Utilizza AWS Config le regole per assicurarti che AMIs vengano utilizzate solo quelle approvate e assicurati che Amazon Inspector sia configurato per scansionare le risorse Amazon ECR alla ricerca di vulnerabilità.

## Best practice correlate nel AWS Well-Architected Framework

- OPS05- BP04 Utilizza sistemi di gestione della compilazione e dell'implementazione
- REL08- BP04 Implementa utilizzando un'infrastruttura immutabile
- SEC06- BP03 Ridurre la gestione manuale e l'accesso interattivo

## Implementazione di questo tema

### Implementa AMI e costruisci pipeline di container

- Usa EC2 Image Builder e integra quanto segue nel tuo: AMIs
  - AWS Systems Manager Agente (SSM Agent), utilizzato ad esempio per il rilevamento e la gestione
  - Strumenti di sicurezza per il controllo delle applicazioni, come Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) () o OpenSCAP GitHub
  - Amazon CloudWatch Agent, utilizzato per la registrazione
- Per tutte le istanze EC2, includi le `AmazonSSMManagedInstanceCore` policy `CloudWatchAgentServerPolicy` e nel profilo dell'istanza o nel ruolo IAM che Systems Manager utilizza per accedere alla tua istanza
- Condividi AMIs con l'intera organizzazione
- Condividi le risorse di EC2 Image Builder
- Assicurati che i team addetti alle applicazioni stiano facendo riferimento alle ultime novità AMIs
- Usa la tua pipeline AMI per la gestione delle patch
- Implementa pipeline di costruzione di container:

  - Crea una pipeline di immagini del contenitore utilizzando la procedura guidata della console EC2 Image Builder
  - Crea una pipeline di distribuzione continua per le immagini dei tuoi container utilizzando Amazon ECR come fonte (AWS post sul blog)
- Condividi le immagini dei container ECR in tutta l'organizzazione tramite architetture multi-account e multiregione

## Implementa pipeline sicure per la creazione di applicazioni

- Implementa pipeline di compilazione per IAc, ad esempio utilizzando EC2 Image AWS CodePipeline Builder e (post sul blog)AWS
- Utilizza strumenti di analisi del codice AWS CloudFormation Guard, come cfn-nag (GitHub) o cdk-nag (GitHub), nelle CI/CD pipeline per rilevare violazioni delle migliori pratiche, come:
  - Politiche IAM troppo permissive, come quelle che utilizzano caratteri jolly
  - Regole dei gruppi di sicurezza troppo permissive, come quelle che utilizzano caratteri jolly o consentono l'accesso SSH
  - Registri di accesso non abilitati
  - Crittografia non abilitata
  - Valori letterali delle password
- Implementa strumenti di scansione nelle pipeline (AWS post sul blog)
- Utilizzalo AWS Identity and Access Management Access Analyzer nelle pipeline (post AWS sul blog) per convalidare le politiche IAM definite nei modelli CloudFormation
- Configura le politiche IAM e le politiche di controllo dei servizi per l'accesso con privilegi minimi per utilizzare la pipeline o apportarvi modifiche

## Implementa la scansione delle vulnerabilità

- Abilita Amazon Inspector in tutti gli account della tua organizzazione
- Usa Amazon Inspector per scansionare la tua AMIs pipeline di compilazione AMI:
  - Gestisci il ciclo di vita delle AMI in EC2 Image Builder () GitHub
- Configura la scansione avanzata per i repository Amazon ECR utilizzando Amazon Inspector
- Crea un programma di gestione delle vulnerabilità per valutare e correggere i problemi di sicurezza

# Monitoraggio di questo tema

## Monitora IAM e log su base continuativa

- Esamina periodicamente le tue politiche IAM per assicurarti che:
  - Solo le pipeline di implementazione hanno accesso diretto alle risorse
  - Solo i servizi approvati hanno accesso diretto ai dati
  - Gli utenti non hanno accesso diretto a risorse o dati
- Monitora AWS CloudTrail i log per confermare che gli utenti stiano modificando le risorse attraverso le pipeline e non stiano modificando direttamente le risorse o accedendo ai dati
- Esamina periodicamente i risultati di IAM Access Analyzer
- Imposta un avviso per avvisarti se vengono utilizzate le credenziali dell'utente root per an Account AWS

## Implementa le seguenti regole AWS Config

- `APPROVED_AMIS_BY_ID`
- `APPROVED_AMIS_BY_TAG`
- `ECR_PRIVATE_IMAGE_SCANNING_ENABLED`

# Tema 3: Gestisci l'infrastruttura mutabile con l'automazione

Otto strategie essenziali coperte

Controllo delle applicazioni, applicazioni di patch, sistemi operativi di patch

Analogamente all'infrastruttura immutabile, l'infrastruttura mutabile viene gestita come IaC e la si modifica o si aggiorna tramite processi automatizzati. Molte delle fasi di implementazione per un'infrastruttura immutabile si applicano anche all'infrastruttura mutabile. Tuttavia, per un'infrastruttura mutabile, è necessario implementare anche controlli manuali per assicurarsi che i carichi di lavoro modificati seguano comunque le migliori pratiche.

Per un'infrastruttura mutabile, è possibile automatizzare la gestione delle patch utilizzando Patch Manager, una funzionalità di. AWS Systems Manager Abilita Patch Manager in tutti gli account della tua AWS organizzazione.

Impedisci l'accesso diretto a SSH e RDP e richiedi agli utenti di utilizzare Session Manager o Run Command, che sono anche funzionalità di Systems Manager. A differenza di SSH e RDP, queste funzionalità possono registrare l'accesso e le modifiche al sistema.

Per monitorare e segnalare la conformità, è necessario eseguire revisioni continue della conformità delle patch. Puoi utilizzare AWS Config le regole per assicurarti che tutte le istanze Amazon EC2 siano gestite da Systems Manager, dispongano delle autorizzazioni richieste e delle applicazioni installate e siano conformi alle patch.

## Best practice correlate nel AWS Well-Architected Framework

- SEC06- BP03 Ridurre la gestione manuale e l'accesso interattivo
- SEC06- BP05 Automatizza la protezione dell'elaborazione

## Implementazione di questo tema

### Automatizza l'applicazione delle patch

- Implementa i passaggi di Enable Patch Manager in tutti gli account della tua organizzazione AWS

- Per tutte le istanze EC2, includi il parametro `CloudWatchAgentServerPolicy` and `AmazonSSMManagedInstanceCore` nel profilo di istanza o nel ruolo IAM che Systems Manager utilizza per accedere all'istanza

## Utilizza l'automazione anziché i processi manuali

- Implementa le linee guida in Implementazione di AMI e pipeline di costruzione di container in Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure
- Utilizza Session Manager o Run Command anziché l'accesso diretto SSH o RDP

## Utilizza l'automazione per installare quanto segue sulle istanze EC2

- AWS Systems Manager Agente (SSM Agent), utilizzato per il rilevamento e la gestione delle istanze
- Strumenti di sicurezza per il controllo delle applicazioni, come Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) () o OpenSCAP GitHub
- Amazon CloudWatch Agent, utilizzato per la registrazione

## Utilizza la revisione tra pari prima di qualsiasi versione per assicurarti che le modifiche soddisfino le migliori pratiche

- Policy IAM troppo permissive, come quelle che utilizzano caratteri jolly
- Regole dei gruppi di sicurezza troppo permissive, come quelle che utilizzano caratteri jolly o consentono l'accesso SSH
- Registri di accesso non abilitati
- Crittografia non abilitata
- Valori letterali delle password
- Politiche IAM sicure

### Utilizza controlli a livello di identità

- Per richiedere agli utenti di modificare le risorse tramite processi automatizzati e impedire la configurazione manuale, consenti le autorizzazioni di sola lettura per i ruoli che gli utenti possono assumere
- Concedi le autorizzazioni per modificare le risorse solo ai ruoli di servizio, come il ruolo utilizzato da Systems Manager

### Implementa la scansione delle vulnerabilità

- Implementa la guida in Implementare la scansione delle vulnerabilità in Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure
- Scansiona le tue istanze EC2 utilizzando Amazon Inspector

## Monitoraggio di questo tema

### Monitora la conformità delle patch su base continuativa

- Segnala la conformità delle patch utilizzando l'automazione e i dashboard
- Implementa un meccanismo per rivedere le dashboard per verificare la conformità delle patch

### Monitora IAM e log su base continuativa

- Esamina periodicamente le tue politiche IAM per assicurarti che:
  - Solo le pipeline di implementazione hanno accesso diretto alle risorse
  - Solo i servizi approvati hanno accesso diretto ai dati
  - Gli utenti non hanno accesso diretto a risorse o dati
- Monitora AWS CloudTrail i log per assicurarti che gli utenti stiano modificando le risorse attraverso le pipeline e non stiano modificando direttamente le risorse o accedendo ai dati
- AWS Identity and Access Management Access Analyzer Esamina periodicamente i risultati
- Imposta un avviso per avvisarti se Account AWS vengono utilizzate le credenziali dell'utente root per an

## Implementa le seguenti regole AWS Config

- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED - SELinux/fapolicyd/OpenSCAP, CW Agent
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED - any unsupported apps
- IAM_ROLE_MANAGED_POLICY_CHECK - CW Logs, SSM
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC - 22, 3389

# Tema 4: Gestire le identità

Le otto strategie essenziali trattate

Limita i privilegi amministrativi, autenticazione a più fattori

Una solida gestione dell'identità e delle autorizzazioni è un aspetto fondamentale della gestione della sicurezza nel cloud. Pratiche solide in materia di identità bilanciano l'accesso necessario e il minimo privilegio. Questo aiuta i team di sviluppo a muoversi rapidamente senza compromettere la sicurezza.

Utilizza la federazione delle identità per centralizzare la gestione delle identità. In questo modo è più semplice gestire l'accesso su più applicazioni e servizi perché si gestisce l'accesso da un'unica posizione. Ciò consente inoltre di implementare autorizzazioni temporanee e autenticazione a più fattori (MFA).

Concedi agli utenti solo le autorizzazioni necessarie per svolgere le proprie attività. AWS Identity and Access Management Access Analyzer può convalidare le politiche e verificare l'accesso pubblico e tra account. Funzionalità come le policy di controllo dei AWS Organizations servizi (SCPs), le condizioni delle policy IAM, i limiti delle autorizzazioni IAM e i set di autorizzazioni possono aiutarti a configurare AWS IAM Identity Center il controllo granulare degli accessi (FGAC).

Quando si esegue qualsiasi tipo di autenticazione, è preferibile utilizzare credenziali temporanee per ridurre o eliminare i rischi, come la divulgazione, la condivisione o il furto inavvertitamente delle credenziali. Utilizza i ruoli IAM anziché gli utenti IAM.

Utilizza meccanismi di accesso efficaci, come l'MFA, per mitigare il rischio che le credenziali di accesso vengano divulgate inavvertitamente o siano facilmente intuibili. Richiedi l'autenticazione MFA per l'utente root e puoi richiederla anche a livello di federazione. Se l'uso di utenti IAM è inevitabile, applica la MFA.

Per monitorare e generare report sulla conformità, è necessario lavorare continuamente per ridurre le autorizzazioni, monitorare i risultati di IAM Access Analyzer e rimuovere le risorse IAM inutilizzate. Utilizza AWS Config le regole per assicurarti che vengano applicati meccanismi di accesso efficaci, che le credenziali abbiano vita breve e che le risorse IAM vengano utilizzate.

# Best practice correlate nel AWS Well-Architected Framework

- SEC02- BP01 Utilizza meccanismi di accesso efficaci
- SEC02- BP02 Usa credenziali temporanee
- SEC02- BP03 Archivia e utilizza i segreti in modo sicuro
- SEC02- BP04 Affidati a un provider di identità centralizzato
- SEC02- BP05 Controlla e ruota periodicamente le credenziali
- SEC02- BP06 Utilizza gruppi e attributi di utenti
- SEC03- BP01 Definire i requisiti di accesso
- SEC03- BP02 Concedi l'accesso con il minimo privilegio
- SEC03- BP03 Stabilire un processo di accesso di emergenza
- SEC03- BP04 Riduci continuamente le autorizzazioni
- SEC03- BP05 Definisci i limiti di autorizzazione per la tua organizzazione
- SEC03- BP06 Gestisci l'accesso in base al ciclo di vita
- SEC03- BP07 Analizza l'accesso pubblico e tra account
- SEC03- BP08 Condividi le risorse in modo sicuro all'interno della tua organizzazione

# Implementazione di questo tema

## Implementare la federazione

- Richiedi agli utenti umani di effettuare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee
- Implementa un accesso temporaneo elevato ai tuoi ambienti AWS

## Applica le autorizzazioni con privilegi minimi

- Proteggi le credenziali dell'utente root e non utilizzarle per le attività quotidiane
- Utilizza IAM Access Analyzer per generare politiche con privilegi minimi basate sull'attività di accesso
- Verifica l'accesso pubblico e tra account alle risorse con IAM Access Analyzer

- Utilizza IAM Access Analyzer per convalidare le tue policy IAM per autorizzazioni sicure e funzionali
- Stabilisci barriere di autorizzazione su più account
- Utilizza i limiti delle autorizzazioni per impostare le autorizzazioni massime che una politica basata sull'identità può concedere
- Utilizza le condizioni nelle policy IAM per limitare ulteriormente l'accesso
- Esamina e rimuovi regolarmente utenti, ruoli, autorizzazioni, politiche e credenziali non utilizzati
- Inizia con le politiche AWS gestite e passa alle autorizzazioni con privilegi minimi
- Utilizza la funzionalità dei set di autorizzazioni in IAM Identity Center

### Ruota le credenziali

- Richiedi ai carichi di lavoro di utilizzare i ruoli IAM per accedere AWS
- Automatizza l'eliminazione dei ruoli IAM non utilizzati
- Ruota regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine

### Applica l'autenticazione a più fattori

- Richiedi MFA per l'utente root
- Richiedi MFA tramite IAM Identity Center
- Prendi in considerazione la possibilità di richiedere l'MFA per azioni API specifiche del servizio

## Monitoraggio di questo tema

### Monitora l'accesso con privilegi minimi

- Invia i risultati di IAM Access Analyzer a AWS Security Hub CSPM
- Prendi in considerazione la possibilità di configurare notifiche per i risultati critici di IAM Identity Center
- Esamina regolarmente i report sulle credenziali per i tuoi Account AWS

## Implementa le seguenti regole AWS Config

- ACCESS_KEYS_ROTATED
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- IAM_PASSWORD_POLICY
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

# Tema 5: Stabilire un perimetro di dati

Otto strategie essenziali trattate

Limita i privilegi amministrativi

Un perimetro di dati è un insieme di barriere preventive nell' AWS ambiente che aiutano a garantire che solo le identità attendibili accedano alle risorse attendibili delle reti previste. Queste barriere fungono da confini sempre attivi che aiutano a proteggere i dati su un'ampia gamma di risorse. Account AWS Queste barriere a livello di organizzazione non sostituiscono i controlli di accesso dettagliati esistenti. Al contrario, aiutano a migliorare la strategia di sicurezza assicurandosi che tutti gli utenti, i ruoli e le risorse AWS Identity and Access Management (IAM) aderiscano a una serie di standard di sicurezza definiti.

È possibile stabilire un perimetro di dati utilizzando politiche che impediscono l'accesso dall'esterno dei confini dell'organizzazione, in genere create in. AWS Organizations Le tre condizioni di autorizzazione perimetrale principali utilizzate per stabilire un perimetro di dati sono:

- Identità affidabili: responsabili (ruoli o utenti IAM) interni all'azienda o che agiscono per conto dell'utente Account AWS. Servizi AWS
- Risorse affidabili: risorse che appartengono a te Account AWS o gestite Servizi AWS agendo per tuo conto.
- Reti previste: i data center locali e i cloud privati virtuali (VPCs) o le reti che Servizi AWS agiscono per conto dell'utente.

Prendi in considerazione l'implementazione di perimetri di dati tra ambienti con diverse classificazioni dei dati, ad esempio `OFFICIAL:SENSITIVE` o`PROTECTED`, o diversi livelli di rischio, come sviluppo, test o produzione. Per ulteriori informazioni, consulta Costruire un perimetro di dati su AWS (AWS white paper) e Stabilire un perimetro di dati su: Panoramica (post di blog). AWSAWS

## Best practice correlate nel AWS Well-Architected Framework

- SEC03- BP05 Definisci i limiti di autorizzazione per la tua organizzazione
- SEC07- BP02 Applica controlli di protezione dei dati basati sulla sensibilità dei dati

# Implementazione di questo tema

## Implementare controlli di identità

- Consenti solo alle identità attendibili di accedere alle tue risorse: utilizza politiche basate sulle risorse con le chiavi di condizione e. `aws:PrincipalOrgID` `aws:PrincipalIsAWSService` Ciò consente solo ai dirigenti della tua AWS organizzazione e di accedere alle AWS tue risorse.
- Consenti identità affidabili solo dalla tua rete: utilizza le policy degli endpoint VPC con le chiavi di condizione e. `aws:PrincipalOrgID` `aws:PrincipalIsAWSService` Ciò consente solo ai responsabili della tua AWS organizzazione e di accedere AWS ai servizi tramite endpoint VPC.

## Implementa controlli sulle risorse

- Consenti alle tue identità di accedere solo a risorse affidabili: utilizza le policy di controllo del servizio (SCPs) con la chiave `aws:ResourceOrgID` di condizione. Ciò consente alle tue identità di accedere solo alle risorse della tua AWS organizzazione.
- Consenti l'accesso a risorse affidabili solo dalla tua rete: utilizza le policy degli endpoint VPC con la chiave di condizione. `aws:ResourceOrgID` Ciò consente alle tue identità di accedere ai servizi solo tramite endpoint VPC che fanno parte della tua organizzazione. AWS

## Implementa controlli di rete

- Consenti alle identità di accedere alle risorse solo dalle reti previste: da utilizzare SCPs con le chiavi di condizione`aws:SourceIp`, `aws:SourceVpc``aws:SourceVpce`, e`aws:ViaAWSService`. Ciò consente alle identità di accedere alle risorse solo dagli indirizzi IP e dagli endpoint VPC previsti e tramite. VPCs Servizi AWS
- Consenti l'accesso alle tue risorse solo dalle reti previste: utilizza politiche basate sulle risorse con le chiavi `aws:SourceIp` di condizione,,, e. `aws:SourceVpc` `aws:SourceVpce` `aws:ViaAWSService` `aws:PrincipalIsAWSService` Ciò consente l'accesso alle risorse solo dagli endpoint VPC previsti VPCs, previsti o previsti Servizi AWS, tramite o quando l'identità chiamante è una. IPs Servizio AWS

# Monitoraggio di questo tema

## Monitora le politiche

- Implementa meccanismi di revisione SCPs delle policy IAM e delle policy degli endpoint VPC

## Implementa le seguenti regole AWS Config

- `SERVICE_VPC_ENDPOINT_ENABLED`

# Tema 6: Automatizza i backup

Otto strategie essenziali coperte

Backup regolari

«I guasti sono un dato di fatto e alla fine tutto fallirà nel tempo: dai router agli hard disk, dai sistemi operativi alle unità di memoria che danneggiano i pacchetti TCP, dagli errori transitori ai guasti permanenti. Questo è un dato di fatto, sia che si utilizzi hardware di altissima qualità o componenti a basso costo». —Werner Vogels, CTO, Amazon, All Things Distributed

Il backup e il ripristino dei dati sono un elemento fondamentale dell'affidabilità di un sistema. AWS è progettato per semplificare la creazione di backup, mantenere la durabilità dei dati di backup e garantire che i dati di backup rimangano recuperabili.

AWS Backupè un servizio completamente gestito che centralizza e automatizza il backup dei dati in tutto il mondo. Servizi AWS Supporta diversi tipi di AWS risorse e aiuta a implementare e mantenere una strategia di backup per i carichi di lavoro che utilizzano più AWS risorse di cui è necessario eseguire il backup collettivamente. AWS Backup consente inoltre di monitorare collettivamente le operazioni di backup e ripristino di più risorse. AWS

AWS Backup Vault Lock è una funzionalità opzionale di un archivio di backup e può fornire sicurezza e controllo aggiuntivi. Quando un blocco è attivo in modalità Compliance e il periodo di prova è scaduto, la configurazione del vault non può essere modificata o eliminata dall'utente, dall'account o dal proprietario dei dati, oppure. AWS Ogni vault può disporre di un solo blocco del vault. Ciò consente la configurazione WORM (Write-Once, Read-Many) e l'applicazione dei periodi di conservazione.

Se si seguono le attuali linee guida di configurazione, è AWS Backup possibile fornire una durabilità annua del 99,99999%, nota anche come 11 nove. Utilizza l'infrastruttura AWS globale per replicare i backup su più zone di disponibilità. Per ulteriori informazioni, consulta Resilienza in AWS Backup.

AWS Backup consente di automatizzare il ripristino e il test dei dati di backup per verificare l'integrità e i processi di backup.

# Best practice correlate nel AWS Well-Architected Framework

- SEC09- BP01 Implementare una gestione sicura di chiavi e certificati
- SEC09- BP02 Applica la crittografia in transito
- SEC09- BP03 Autentica le comunicazioni di rete

# Implementazione di questo tema

## Automatizza il backup e il ripristino dei dati

- Implementa il backup dei dati su AWS
- Automatizza il backup dei dati su larga scala (post AWS sul blog)
- Automatizza la convalida del ripristino dei dati con AWS Backup (AWS post sul blog)

## Implementa la governance in tutti i tuoi risultati AWS Backup

- Le 10 migliori pratiche di sicurezza per proteggere i backup in AWS (AWS post sul blog)
- Usa AWS Backup Vault Lock per migliorare la sicurezza delle tue casseforti di backup
- Usa AWS Backup Audit Manager per verificare la conformità delle tue AWS Backup politiche

# Monitoraggio di questo tema

## Implementa le seguenti AWS Config regole

- `RDS_IN_BACKUP_PLAN`
- `RDS_LAST_BACKUP_RECOVERY_POINT_CREATED`
- `RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN`
- `REDSHIFT_BACKUP_ENABLED`
- `AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED`
- `AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN`
- `BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK`
- `BACKUP_RECOVERY_POINT_ENCRYPTED`

- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- DB_INSTANCE_BACKUP_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

# Tema 7: Centralizzare la registrazione e il monitoraggio

> Otto strategie essenziali trattate
>
> Controllo delle applicazioni, applicazione di patch, limitazione dei privilegi amministrativi, autenticazione a più fattori

AWS fornisce strumenti e funzionalità che consentono di vedere cosa succede nel proprio AWS ambiente. Ciò include:

- AWS CloudTrailti aiuta a monitorare le tue AWS implementazioni creando una cronologia delle chiamate AWS API per il tuo account, incluse le chiamate API effettuate tramite gli strumenti Console di gestione AWS a riga di comando e. AWS SDKs Per i servizi che supportano CloudTrail, puoi anche identificare quali utenti e account hanno chiamato l'API del servizio, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono state effettuate le chiamate.
- Amazon ti CloudWatch aiuta a monitorare i parametri delle tue AWS risorse e delle applicazioni su cui esegui AWS in tempo reale.
- Amazon CloudWatch Logs ti aiuta a centralizzare i log di tutti i tuoi sistemi e applicazioni, Servizi AWS così puoi monitorarli e archiviarli in modo sicuro.
- Amazon GuardDuty è un servizio di monitoraggio continuo della sicurezza che analizza ed elabora i log per identificare attività impreviste e potenzialmente non autorizzate nel tuo ambiente. AWS GuardDuty si integra con Amazon EventBridge per avviare una risposta automatica o avvisare un essere umano.
- AWS Security Hub CSPMfornisce una visione completa del tuo stato di sicurezza in AWS. Inoltre, consente di verificare la conformità AWS dell'ambiente agli standard e alle best practice del settore della sicurezza.

Questi strumenti e funzionalità sono progettati per aumentare la visibilità e aiutarti a risolvere i problemi prima che influiscano negativamente sull'ambiente. Ciò consente di migliorare il livello di sicurezza dell'organizzazione nel cloud e riduce il profilo di rischio dell'ambiente.

## Best practice correlate nel AWS Well-Architected Framework

- SEC04- BP01 Configurazione della registrazione dei servizi e delle applicazioni

- SEC04- BP02 Acquisisci registri, risultati e metriche in posizioni standardizzate

# Implementazione di questo tema

## Enable logging (Attiva registrazione)

- Utilizza l' CloudWatch agente per pubblicare i log a livello di sistema in Logs CloudWatch
- Imposta avvisi per i risultati GuardDuty
- Crea un percorso organizzativo in CloudTrail

## Implementa le migliori pratiche di sicurezza per la registrazione

- Implementa le migliori CloudTrail pratiche di sicurezza
- Da utilizzare SCPs per impedire agli utenti di disabilitare i servizi di sicurezza (post AWS sul blog)
- Crittografa i dati di registro in CloudWatch Logs utilizzando AWS Key Management Service

## Centralizza i log

- Ricevi i CloudTrail log da più account
- Invia i registri a un account di archiviazione dei registri
- Centralizza CloudWatch i log in un account per il controllo e l'analisi (post sul blog)AWS
- Gestione centralizzata di Amazon Inspector
- Crea un aggregatore per tutta l'organizzazione in (post del blog) AWS ConfigAWS
- Gestione centralizzata del Security Hub CSPM
- Centralizza la gestione di GuardDuty
- Prendi in considerazione l'utilizzo di Amazon Security Lake

# Monitoraggio di questo tema

## Implementare meccanismi

- Stabilisci un meccanismo per esaminare i risultati dei log
- Stabilire un meccanismo per esaminare i risultati del Security Hub CSPM

- Stabilisci un meccanismo per rispondere ai risultati GuardDuty

## Implementa le seguenti AWS Config regole

- `CLOUDTRAIL_SECURITY_TRAIL_ENABLED`
- `GUARDDUTY_ENABLED_CENTRALIZED`
- `SECURITYHUB_ENABLED`
- `ACCOUNT_PART_OF_ORGANIZATIONS`

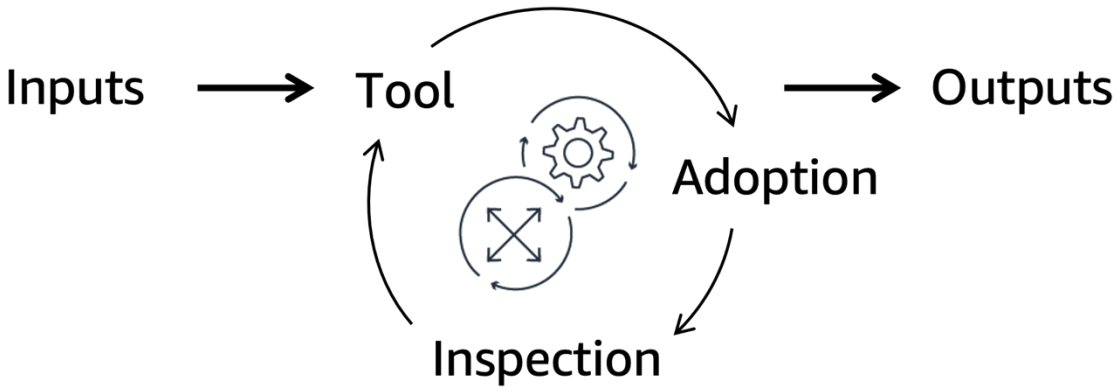
# Tema 8: Implementazione di meccanismi per i processi manuali

Sono state trattate le otto strategie essenziali

Controllo delle applicazioni, applicazioni di patch

In Amazon, abbiamo un detto: le buone intenzioni non funzionano, i meccanismi sì (AWS post sul blog). Ciò significa che è necessario sostituire i migliori sforzi con processi e strumenti automatizzati, ripetibili e scalabili per ottenere i risultati desiderati.

Come illustrato nel diagramma seguente, un meccanismo è un processo completo in cui si crea uno strumento, si promuove l'adozione dello strumento e quindi si esaminano i risultati per apportare modifiche. È un ciclo che si rafforza e si migliora man mano che funziona. Prende input controllabili e li trasforma in output continui per affrontare una sfida aziendale ricorrente. Per ulteriori informazioni, consulta Creazione di meccanismi nel AWS Well-Architected Framework.




## Best practice correlate nel AWS Well-Architected Framework

- OPS02- BP01 Le risorse hanno identificato i proprietari
- OPS02- BP02 I processi e le procedure hanno identificato i proprietari
- OPS02- BP03 Le attività operative hanno identificato i proprietari responsabili delle loro prestazioni
- OPS02- Esistono BP04 meccanismi per gestire le responsabilità e la proprietà
- OPS03- BP01 Fornire una sponsorizzazione esecutiva

- OPS03- L'BP03 escalation è incoraggiata

## Implementazione di questo tema

- Stabilisci meccanismi per esaminare e risolvere le lacune di conformità
- Stabilisci meccanismi per aggiornare le politiche di sicurezza
- Rimuovi le applicazioni che non sono supportate e aggiungile all'elenco delle AWS Config regole negate
- Convalida le politiche di accesso con AWS Identity and Access Management Access Analyzer
- Abilita Amazon Inspector, che conserva automaticamente i registri delle vulnerabilità up-to-date
- Rivedi almeno una volta all'anno i set di regole di controllo delle applicazioni
- Prendi in considerazione l'implementazione dell'automazione, ad esempio AWS Config le regole, per ridurre il carico dei processi manuali
- Prendi in considerazione l'utilizzo di AWS Systems Manager Inventory per ottenere visibilità su quali istanze eseguono il software richiesto dalla tua politica software

## Monitoraggio di questo tema

- Stabilisci la supervisione degli sponsor esecutivi in modo che possano monitorare i progressi verso gli obiettivi, tra cui la conformità, l'ispezione delle lacune e la valutazione dei meccanismi.

# Caso di studio indicativo per raggiungere la maturità di Essential Eight su AWS

Questo capitolo presenta un case study indicativo per un'agenzia governativa che punta alla maturità di Essential Eight. AWS

Sezioni di questo capitolo:

- Panoramica dello scenario e dell'architettura
- Esempio di carico di lavoro: data lake senza server
- Esempio di carico di lavoro: servizio web containerizzato
- Esempio di carico di lavoro: software COTS su Amazon EC2

## Panoramica dello scenario e dell'architettura

L'agenzia governativa ha tre carichi di lavoro nei seguenti settori: Cloud AWS

- Un data lake serverless che utilizza Amazon Simple Storage Service (Amazon S3) per lo storage e AWS Lambda per le operazioni di estrazione, trasformazione e caricamento (ETL)
- Un servizio Web containerizzato che viene eseguito su Amazon Elastic Container Service (Amazon ECS) e utilizza un database in Amazon Relational Database Service (Amazon RDS)
- Un software commerciale off-the-shelf (COTS) in esecuzione su Amazon EC2

Un team cloud fornisce una piattaforma centralizzata per l'organizzazione, che gestisce i servizi di base per l'ambiente. AWS Un team cloud fornisce i servizi di base per l' AWS ambiente. Ogni carico di lavoro è di proprietà di un team applicativo distinto, noto anche come team di sviluppo o team di consegna.

### Architettura di base

Il team cloud ha già stabilito le seguenti funzionalità in Cloud AWS:

- La federazione delle identità si collega AWS IAM Identity Center alla relativa istanza Microsoft Entra ID (in precedenza Azure Active Directory). La federazione applica la MFA, la scadenza automatica degli account utente e l'uso di credenziali AWS Identity and Access Management di breve durata tramite ruoli (IAM).

- Una pipeline AMI centralizzata viene utilizzata per applicare patch ai sistemi operativi e alle applicazioni principali con EC2 Image Builder.
- Amazon Inspector è abilitato a identificare le vulnerabilità e tutti i risultati di sicurezza vengono inviati ad Amazon GuardDuty per la gestione centralizzata.
- Vengono utilizzati meccanismi consolidati per aggiornare le regole di controllo delle applicazioni, rispondere agli eventi di sicurezza informatica e esaminare le lacune di conformità.
- AWS CloudTrail viene utilizzato per la registrazione e il monitoraggio.
- Gli eventi di sicurezza, come l'accesso dell'utente root, avviano gli avvisi.
- SCPs e le policy degli endpoint VPC stabiliscono i perimetri dei dati per i tuoi ambienti. AWS
- SCPs impedisci ai team addetti alle applicazioni di disabilitare i servizi di sicurezza e registrazione, come e. CloudTrail AWS Config
- AWS Config i risultati vengono aggregati dall'intera AWS organizzazione in un unico Account AWS documento per motivi di sicurezza.
- Il pacchetto di conformità AWS Config ACSC Essential 8 è abilitato in tutta Account AWS l'organizzazione.

## Esempio di carico di lavoro: data lake senza server

Questo carico di lavoro è un esempio di. Tema 1: Utilizzare i servizi gestiti

Il data lake utilizza Amazon S3 per lo storage e AWS Lambda per ETL. Queste risorse sono definite in un' AWS Cloud Development Kit (AWS CDK) app. Le modifiche al sistema vengono implementate tramite AWS CodePipeline. Questa pipeline è limitata al team dell'applicazione. Quando il team dell'applicazione effettua una pull request per l'archivio del codice, viene utilizzata la regola delle due persone.

Per questo carico di lavoro, il team dell'applicazione intraprende le seguenti azioni per affrontare le strategie Essential Eight.

Controllo delle applicazioni

- Il team dell'applicazione abilita la protezione Lambda e la scansione GuardDuty Lambda in Amazon Inspector.
- Il team applicativo implementa meccanismi per ispezionare e gestire i risultati di Amazon Inspector.

Applicazioni di patch

- Il team dell'applicazione abilita la scansione Lambda in Amazon Inspector e configura gli avvisi per le librerie obsolete o vulnerabili.
- Il team dell'applicazione consente AWS Config di tenere traccia delle risorse per l'individuazione delle risorse. AWS

Limita i privilegi amministrativi

- Come descritto nella Architettura di base sezione, il team dell'applicazione limita già l'accesso alle distribuzioni di produzione mediante una regola di approvazione sulla relativa pipeline di distribuzione.
- Il team dell'applicazione si affida alla federazione centralizzata delle identità e alle soluzioni di registrazione centralizzate descritte nella sezione. Architettura di base
- Il team dell'applicazione crea un AWS CloudTrail percorso e CloudWatch filtri Amazon.
- Il team dell'applicazione configura gli avvisi di Amazon Simple Notification Service (Amazon SNS) CodePipeline per le distribuzioni e le eliminazioni di stack. AWS CloudFormation

Patch i sistemi operativi

- Il team dell'applicazione abilita la scansione Lambda in Amazon Inspector e configura gli avvisi per le librerie obsolete o vulnerabili.

Autenticazione a più fattori

- Il team dell'applicazione si affida alla soluzione centralizzata di federazione delle identità descritta nella sezione. Architettura di base Questa soluzione applica l'MFA, registra le autenticazioni e gli avvisi o risponde automaticamente a eventi MFA sospetti.

Backup regolari

- Il team dell'applicazione archivia il codice, ad esempio AWS CDK app e funzioni e configurazioni Lambda, in un repository di codice.
- Il team dell'applicazione abilita il controllo delle versioni e Amazon S3 Object Lock per impedire l'eliminazione o la modifica degli oggetti.
- Il team dell'applicazione si affida alla durabilità integrata di Amazon S3 anziché replicare l'intero set di dati su un altro. Regione AWS

- Il team dell'applicazione esegue una copia del carico di lavoro in un altro Regione AWS che soddisfa i requisiti di sovranità dei dati. Utilizzano le tabelle globali di Amazon DynamoDB e Amazon S3 Cross-Region Replication per replicare automaticamente i dati dalla regione primaria alla regione secondaria.

## Esempio di carico di lavoro: servizio web containerizzato

Questo carico di lavoro è un esempio di. Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure

Il servizio Web viene eseguito su Amazon ECS e utilizza un database in Amazon RDS. Il team dell'applicazione definisce queste risorse in un CloudFormation modello. I contenitori vengono creati con EC2 Image Builder e archiviati in Amazon ECR. Il team dell'applicazione implementa le modifiche al sistema tramite. AWS CodePipeline Questa pipeline è limitata al team dell'applicazione. Quando il team dell'applicazione effettua una pull request per l'archivio del codice, viene utilizzata la regola delle due persone.

Per questo carico di lavoro, il team dell'applicazione intraprende le seguenti azioni per affrontare le strategie Essential Eight.

Controllo delle applicazioni

- Il team dell'applicazione consente la scansione delle immagini dei container Amazon ECR in Amazon Inspector.
- Il team dell'applicazione crea lo strumento di sicurezza File Access Policy Daemon (fapolicyd) nella pipeline EC2 Image Builder. Per ulteriori informazioni, consulta Implementing Application Control sul sito Web ACSC.
- Il team dell'applicazione configura la definizione del task di Amazon ECS per registrare l'output su Amazon CloudWatch Logs.
- Il team applicativo implementa meccanismi per ispezionare e gestire i risultati di Amazon Inspector.

Applicazioni di patch

- Il team dell'applicazione consente la scansione delle immagini dei container Amazon ECR in Amazon Inspector e configura gli avvisi per le librerie obsolete o vulnerabili.

- Il team applicativo automatizza le risposte ai risultati di Amazon Inspector. Le nuove scoperte avviano la loro pipeline di implementazione tramite un EventBridge trigger di Amazon, ed CodePipeline è l'obiettivo.
- Il team dell'applicazione consente di AWS Config tenere traccia AWS delle risorse per l'individuazione delle risorse.

Limita i privilegi amministrativi

- Il team addetto all'applicazione sta già limitando l'accesso alle implementazioni di produzione mediante una regola di approvazione sulla relativa pipeline di distribuzione.
- Il team addetto all'applicazione si affida alla federazione delle identità del team cloud centralizzato per la rotazione delle credenziali e la registrazione centralizzata.
- Il team dell'applicazione crea un percorso e filtri. CloudTrail CloudWatch
- Il team applicativo configura gli avvisi di Amazon SNS per le CodePipeline distribuzioni e le eliminazioni di stack. CloudFormation

Patch i sistemi operativi

- Il team dell'applicazione consente la scansione delle immagini dei container Amazon ECR in Amazon Inspector e configura gli avvisi per gli aggiornamenti delle patch del sistema operativo.
- Il team addetto all'applicazione automatizza la risposta ai risultati di Amazon Inspector. Le nuove scoperte avviano la loro pipeline di implementazione tramite un EventBridge trigger e CodePipeline costituiscono l'obiettivo.
- Il team dell'applicazione si iscrive alle notifiche degli eventi di Amazon RDS in modo da essere informato sugli aggiornamenti. Prendono una decisione basata sul rischio con il titolare dell'attività se applicare questi aggiornamenti manualmente o lasciare che Amazon RDS li applichi automaticamente.
- Il team dell'applicazione configura l'istanza Amazon RDS come cluster Multi-Availability Zone al fine di ridurre l'impatto degli eventi di manutenzione.

Autenticazione a più fattori

- Il team dell'applicazione si affida alla soluzione centralizzata di federazione delle identità descritta nella sezione. Architettura di base Questa soluzione applica l'MFA, registra le autenticazioni e gli avvisi o risponde automaticamente a eventi MFA sospetti.

Backup regolari

- Il team dell'applicazione si configura AWS Backup per automatizzare il backup dei dati nel proprio cluster Amazon RDS.
- Il team dell'applicazione archivia i CloudFormation modelli in un repository di codice.
- Il team dell'applicazione sviluppa una pipeline automatizzata per creare una copia del carico di lavoro in un'altra regione ed eseguire test automatici (AWS post sul blog). Dopo l'esecuzione dei test automatici, la pipeline distrugge lo stack. Questa pipeline viene eseguita automaticamente una volta al mese e convalida l'efficacia delle procedure di ripristino.

## Esempio di carico di lavoro: software COTS su Amazon EC2

Questo carico di lavoro è un esempio di. Tema 3: Gestisci l'infrastruttura mutabile con l'automazione

Il carico di lavoro in esecuzione su Amazon EC2 è stato creato manualmente utilizzando. Console di gestione AWS Gli sviluppatori aggiornano manualmente il sistema accedendo alle istanze EC2 e aggiornando il software.

Per questo carico di lavoro, i team del cloud e delle applicazioni intraprendono le seguenti azioni per affrontare le strategie Essential Eight.

Controllo delle applicazioni

- Il team cloud configura la propria pipeline AMI centralizzata per installare e configurare AWS Systems Manager l'agente (agente SSM), CloudWatch l'agente e. SELinux Condividono l'AMI risultante tra tutti gli account dell'organizzazione.
- Il team cloud utilizza AWS Config le regole per confermare che tutte le istanze EC2 in esecuzione siano gestite da Systems Manager e abbiano un agente, CloudWatch un agente e un'installazione SSM. SELinux
- Il team cloud invia l'output di Amazon CloudWatch Logs a una soluzione SIEM (Security Information and Event Management) centralizzata che funziona su Amazon Service. OpenSearch
- Il team applicativo implementa meccanismi per ispezionare e gestire i risultati da e per AWS Config Amazon GuardDuty Inspector. Il team cloud implementa i propri meccanismi per catturare eventuali risultati non rilevati dal team applicativo. Per ulteriori indicazioni sulla creazione di un programma di gestione delle vulnerabilità per risolvere i problemi, consulta Building a scalable vulnerability management program on. AWS

Applicazioni di patch

- Il team dell'applicazione applica le patch alle istanze in base ai risultati di Amazon Inspector.
- Il team cloud applica le patch all'AMI di base e il team dell'applicazione riceve un avviso quando l'AMI cambia.
- Il team dell'applicazione limita l'accesso diretto alle proprie istanze EC2 configurando le regole del gruppo di sicurezza per consentire il traffico solo sulle porte richieste dal carico di lavoro.
- Il team dell'applicazione utilizza Patch Manager per applicare patch alle istanze anziché accedere alle singole istanze.
- Per eseguire comandi arbitrari su gruppi di istanze EC2, il team dell'applicazione utilizza Run Command.
- Nelle rare occasioni in cui il team dell'applicazione necessita dell'accesso diretto a un'istanza, utilizza Session Manager. Questo approccio di accesso utilizza identità federate e registra qualsiasi attività di sessione a fini di controllo.

Limita i privilegi amministrativi

- Il team dell'applicazione configura le regole dei gruppi di sicurezza per consentire il traffico solo sulle porte richieste dal carico di lavoro. Ciò limita l'accesso diretto alle istanze Amazon EC2 e richiede che gli utenti accedano alle istanze EC2 tramite Session Manager.
- Il team applicativo si affida alla federazione delle identità del team cloud centralizzato per la rotazione delle credenziali e la registrazione centralizzata.
- Il team dell'applicazione crea un percorso e filtri. CloudTrail CloudWatch
- Il team applicativo configura gli avvisi di Amazon SNS per le CodePipeline distribuzioni e le eliminazioni di stack. CloudFormation

Patch i sistemi operativi

- Il team cloud applica le patch all'AMI di base e il team dell'applicazione riceve un avviso quando l'AMI cambia. Il team dell'applicazione distribuisce nuove istanze utilizzando questa AMI, quindi utilizza State Manager, una funzionalità di Systems Manager, per installare il software richiesto.
- Il team dell'applicazione utilizza Patch Manager per applicare patch alle istanze, ad esempio per l'accesso a singole istanze.
- Per eseguire comandi arbitrari su gruppi di istanze EC2, il team dell'applicazione utilizza Run Command.

- Nelle rare occasioni in cui il team dell'applicazione necessita di un accesso diretto, utilizza Session Manager.

Autenticazione a più fattori

- Il team dell'applicazione si affida alla soluzione centralizzata di federazione delle identità descritta nella Architettura di base sezione. Questa soluzione applica l'MFA, registra le autenticazioni e gli avvisi o risponde automaticamente a eventi MFA sospetti.

Backup regolari

- Il team applicativo crea un AWS Backup piano per le sue istanze EC2 e i volumi Amazon Elastic Block Store (Amazon EBS).
- Il team dell'applicazione implementa un meccanismo per eseguire manualmente un ripristino del backup ogni mese.

# Risorse

## AWS documentazione

- AWS Architettura di riferimento per la sicurezza (AWS SRA)
- AWS documentazione sulla sicurezza
- Il pilastro della sicurezza del AWS Well-Architected Framework

## Altre risorse AWS

- AWS Sicurezza nel cloud
- AWS Cloud Adoption Framework (prospettiva di sicurezza)

## Risorse dell'Australian Cyber Security Center

- Essential Eight spiegato
- Modello Essential Eight Maturity
- Guida al processo di valutazione Essential Eight

# Collaboratori

Hanno collaborato alla stesura del presente documento:

- James Kingsmill, Senior Solutions Architect, Solutions Architecture AWS
- Chris Harding, Architetto delle soluzioni senior, Architettura delle soluzioni AWS
- Jess Modini, architetto di soluzioni consultive, architettura delle soluzioni AWS
- Justin Bowden, responsabile della garanzia della sicurezza, garanzia della sicurezza AWS
- Rob Powell, Senior Solutions Architect, Solutions Architecture AWS
- Tony Mihaljevic, Senior Cloud Architect, Servizi professionali AWS
- Volker Rath, consulente principale per la sicurezza, Global Services Security AWS

# Appendice: Otto matrici di controllo essenziali

Le tabelle seguenti collegano le strategie Essential Eight alle linee guida AWS all'implementazione e alle migliori pratiche pertinenti nel AWS Well-Architected Framework. Per i controlli Essential Eight che non sono applicabili in Cloud AWS, la tabella include un collegamento a linee guida aggiuntive dell'Australian Cyber Security Centre (ACSC).

Matrici di controllo:

- Controllo delle applicazioni
- Applicazioni di patch
- Configura le impostazioni delle macro Microsoft Office
- Rafforzamento delle applicazioni utente
- Limita i privilegi amministrativi
- Patch i sistemi operativi
- Autenticazione a più fattori
- Backup regolari

## Controllo delle applicazioni

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Il controllo delle applicazioni viene implementato su workstation e server per limitare l'esecuzione di file eseguibili, librerie software, script, programmi di installazione, HTML compilati, applicazioni HTML, applet e driver del pannello | Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementazione di AMI e pipeline di creazione di container | Usa EC2 Image Builder e integra:<br>• AWS Systems Manager Agente (agente SSM)<br>• Strumenti di sicurezza per il controllo delle applicazioni, come Security Enhanced Linux (SELinux) | SEC06- BP02 Fornisci il calcolo a partire da immagini protette |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| di controllo a un set approvato dall'organizzazione. | | (GitHub), File Access Policy Daemon (fapolicyd) () o OpenSCAP GitHub<br><br>CloudWatch Agente Amazon<br><br>Condividi AMIs con l'intera organizzazione<br><br>Assicurati che i team addetti all'applicazione stiano facendo riferimento alle ultime novità AMIs<br><br>Usa la tua pipeline AMI per la gestione delle patch | |
| Microsoftsono implementate le «regole di blocco consigliate». | Vedi Implementing Application Control (sito web ACSC) | Non applicabile | Non applicabile |
| Microsoftsono implementate le «regole consigliate per il blocco dei driver». | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| I set di regole per il controllo delle applicazioni vengono convalidati su base annuale o più frequente. | Tema 8: Implementazione di meccanismi per i processi manuali: Implementazione di un meccanismo per aggiornare le politiche di sicurezza | Non disponibile | SEC01- BP08 Valuta e implementa regolarmente nuovi servizi e funzionalità di sicurezza |
| Le esecuzioni consentite e bloccate su workstation e server vengono registrate centralmente e protette da modifiche ed eliminazioni non autorizzate, monitorate per rilevare eventuali segni di compromissione e intervenute quando vengono rilevati eventi di sicurezza informatica. | Tema 7: Centralizzare la registrazione e il monitoraggio: Abilita la registrazione | Utilizza l' CloudWatch agente per pubblicare i log a livello di sistema in Logs CloudWatch<br><br>Imposta avvisi per i risultati GuardDuty<br><br>Crea un percorso organizzativo in CloudTrail<br><br>Proteggi i dati archiviati in Amazon S3 utilizzando il controllo delle versioni e S3 Object Lock | SEC04- BP01 Configura la registrazione di servizi e applicazioni<br><br>SEC04- BP02 Acquisisci registri, risultati e metriche in posizioni standardizzate |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| | Tema 7: Centralizzare la registrazione e il monitoraggio: Implementa le migliori pratiche di sicurezza della registrazione | Implementa le migliori CloudTrail pratiche di sicurezza<br><br>Da utilizzare SCPs per impedire agli utenti di disabilitare i servizi di sicurezza (post AWS sul blog)<br><br>Crittografa i dati di registro in CloudWatch Logs utilizzando AWS Key Management Service | SEC04- BP01 Configura la registrazione dei servizi e delle applicazioni<br><br>SEC04- BP02 Acquisisci registri, risultati e metriche in posizioni standardizzate |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| | Tema 7: Centralizzare la registrazione e il monitoraggio: Centralizza i log | Ricevi CloudTrail registri da più account<br><br>Invia i registri a un account di archiviazione dei registri<br><br>Centralizza CloudWatch i log in un account per il controllo e l'analisi (post sul blog)AWS<br><br>Gestione centralizzata di Amazon Inspector<br><br>Crea un aggregatore per tutta l'organizzazione in (post del blog) AWS ConfigAWS<br><br>Gestione centralizzata del Security Hub CSPM<br><br>Centralizza la gestione di GuardDuty<br><br>Prendi in considerazione l'utilizzo di Amazon Security Lake | SEC04- BP02 Acquisisci log, risultati e metriche in posizioni standardizzate |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| | Tema 8: Implementazione di meccanismi per i processi manuali: Implementazione di meccanismi per esaminare e risolvere le lacune di conformità | Prendi in considerazione l'implementazione dell'automazione, ad esempio AWS Config le regole, per ridurre il carico dei processi manuali | OPS02- BP02 I processi e le procedure hanno identificato i proprietari<br><br>OPS02- BP03 Le attività operative hanno identificato i proprietari responsabili delle loro prestazioni<br><br>OPS02- Esistono BP04 meccanismi per gestire le responsabilità e la proprietà |

## Applicazioni di patch

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Un metodo automatizzato di rilevamento delle risorse viene utilizzato almeno ogni due settimane per supportare il rilevamento delle risorse per le successive attività | Tema 1: Utilizzare i servizi gestiti: Scansiona le vulnerabilità<br><br>Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementa la | Abilita Amazon Inspector in tutti gli account della tua organizzazione<br><br>Configura la scansione avanzata per i repository Amazon ECR utilizzando Amazon Inspector | SEC06- BP01 Esegui la gestione delle vulnerabilità<br><br>SEC06- BP05 Automatizza la protezione dell'elaborazione |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
| --- | --- | --- | --- |
| di scansione delle vulnerabilità. | scansione delle vulnerabilità<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Implementazione della scansione delle vulnerabilità | Crea un programma di gestione delle vulnerabilità per valutare e correggere i problemi di sicurezza | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| | Tema 7: Centralizzare la registrazione e il monitoraggio: Centralizza i log | Ricevi CloudTrail registri da più account<br><br>Invia i registri a un account di archiviazione dei registri<br><br>Centralizza CloudWatch i log in un account per il controllo e l'analisi (post sul blog)AWS<br><br>Gestione centralizzata di Amazon Inspector<br><br>Crea un aggregatore per tutta l'organizzazione in (post del blog) AWS ConfigAWS<br><br>Gestione centralizzata del Security Hub CSPM<br><br>Centralizza la gestione di GuardDuty<br><br>Prendi in considerazione l'utilizzo di Security Lake | SEC04- BP02 Acquisisci registri, risultati e metriche in posizioni standardizzate |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Per le attività di scansione delle vulnerabilità viene utilizzato uno scanner up-to-date di vulnerabilità con un database di vulnerabilità. | Tema 1: Utilizzare i servizi gestiti: Scansiona le vulnerabilità<br><br>Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementa la scansione delle vulnerabilità<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Implementazione della scansione delle vulnerabilità | Abilita Amazon Inspector in tutti gli account della tua organizzazione<br><br>Configura la scansione avanzata per i repository Amazon ECR utilizzando Amazon Inspector<br><br>Crea un programma di gestione delle vulnerabilità per valutare e correggere i problemi di sicurezza | SEC06- BP01 Esegui la gestione delle vulnerabilità<br><br>SEC06- BP05 Automatizza la protezione dell'elaborazione |
| Uno scanner di vulnerabilità viene utilizzato almeno quotidianamente per identificare le patch o gli aggiornamenti mancanti per le vulnerabilità di sicurezza nei servizi connessi a Internet. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Uno scanner di vulnerabilità viene utilizzato almeno una volta alla settimana per identificare le patch o gli aggiornamenti mancanti per le vulnerabilità di sicurezza nelle suite di produttività per ufficio, nei browser Web e nelle relative estensioni, nei client di posta elettronica, nei software PDF e nei prodotti di sicurezza. | Vedi Esempio tecnico: applicazioni di patch (sito Web ACSC) | Non applicabile | Non applicabile |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Uno scanner di vulnerabilità viene utilizzato almeno ogni due settimane per identificare le patch o gli aggiornamenti mancanti relativi alle vulnerabilità di sicurezza in altre applicazioni. | Tema 1: Utilizzare i servizi gestiti: Scansione per individuare eventuali vulnerabilità<br><br>Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementa la scansione delle vulnerabilità<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Implementazione della scansione delle vulnerabilità | Abilita Amazon Inspector in tutti gli account della tua organizzazione<br><br>Configura la scansione avanzata per i repository Amazon ECR utilizzando Amazon Inspector<br><br>Crea un programma di gestione delle vulnerabilità per valutare e correggere i problemi di sicurezza | SEC06- BP01 Esegui la gestione delle vulnerabilità<br><br>SEC06- BP05 Automatizza la protezione dell'elaborazione |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le patch, gli aggiornamenti o le mitigazioni dei fornitori per le vulnerabilità di sicurezza nei servizi connessi a Internet vengono applicati entro due settimane dal rilascio o entro 48 ore se esiste un exploit. | Tema 1: Utilizzare i servizi gestiti: Scansione per individuare eventuali vulnerabilità<br><br>Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementa la scansione delle vulnerabilità<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Implementazione della scansione delle vulnerabilità | Abilita Amazon Inspector in tutti gli account della tua organizzazione<br><br>Configura la scansione avanzata per i repository Amazon ECR utilizzando Amazon Inspector<br><br>Crea un programma di gestione delle vulnerabilità per valutare e correggere i problemi di sicurezza | SEC06- BP01 Esegui la gestione delle vulnerabilità |
| | Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Automatizza l'applicazione delle patch | Abilita Patch Manager in tutti gli account della tua organizzazione AWS | SEC06- BP01 Esegui la gestione delle vulnerabilità<br><br>SEC06- BP05 Automatizza la protezione dell'elaborazione |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le patch, gli aggiornamenti o le mitigazioni dei fornitori per le vulnerabilità di sicurezza nelle suite di produttività per ufficio, nei browser Web e nelle relative estensioni, nei client di posta elettronica, nel software PDF e nei prodotti di sicurezza vengono applicati entro due settimane dal rilascio o entro 48 ore se esiste un exploit. | Vedi Esempio tecnico: applicazioni di patch (sito web ACSC) | Non applicabile | Non applicabile |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le patch, gli aggiornamenti o le mitigazioni dei fornitori per le vulnerabilità di sicurezza in altre applicazioni vengono applicate entro un mese dal rilascio. | Tema 1: Utilizzare i servizi gestiti: Scansiona le vulnerabilità<br><br>Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementa la scansione delle vulnerabilità<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Implementazione della scansione delle vulnerabilità | Abilita Amazon Inspector in tutti gli account della tua organizzazione<br><br>Configura la scansione avanzata per i repository Amazon ECR utilizzando Amazon Inspector<br><br>Crea un programma di gestione delle vulnerabilità per valutare e correggere i problemi di sicurezza | SEC06- BP01 Esegui la gestione delle vulnerabilità |
| | Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Automatizza l'applicazione delle patch | Abilita Patch Manager in tutti gli account della tua organizzazione AWS | SEC06- BP01 Esegui la gestione delle vulnerabilità<br><br>SEC06- BP05 Automatizza la protezione dell'elaborazione |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le applicazioni che non sono più supportate dai fornitori vengono rimosse. | Tema 8: Implementazione di meccanismi per i processi manuali: Implementazione di meccanismi per esaminare e risolvere le lacune di conformità | Prendi in considerazione l'utilizzo di AWS Systems Manager Inventory per ottenere visibilità su quali istanze eseguono il software richiesto dalla tua politica software | SEC06- BP02 Fornisci elaborazione a partire da immagini protette |

## Configura le impostazioni delle macro Microsoft Office

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Microsoft Officele macro sono disattivate per gli utenti che non hanno un requisito aziendale comprovato. | Vedi Esempio tecnico: Configurazione delle impostazioni delle macro (sito Web ACSC) | Non applicabile | Non applicabile |
| È consentita l'esecuzione solo delle Microsoft Office macro eseguite da un ambiente in modalità sandbox, da una posizione attendibile o che sono firmate digitalmente da un editore attendibile. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Solo gli utenti privilegiati responsabili della verifica dell'assenza di codice dannoso nelle Microsoft Office macro possono scrivere e modificare il contenuto all'interno di Trusted Locations. | | | |
| Microsoft Officele macro firmate digitalmente da un editore non attendibile non possono essere abilitate tramite la barra dei messaggi o la visualizzazione Backstage. | | | |
| Microsoft Officel'e lenco di editori attendibili viene convalidato su base annuale o più frequente. | | | |
| Microsoft Officele macro nei file provenienti da Internet sono bloccate. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Microsoft Officela scansione macro antivirus è abilitata. | | | |
| Microsoft Officealle macro viene impedito di effettuare chiamate Win32 API. | | | |
| Microsoft Officele impostazioni di protezione delle macro non possono essere modificate dagli utenti. | | | |
| Le esecuzioni di Microsoft Office macro consentite e bloccate vengono registrate centralmente e protette da modifiche ed eliminazioni non autorizzate, monitorate per rilevare eventuali segni di compromissione e intervenute quando vengono rilevati eventi di sicurezza informatica. | | | |

# Rafforzamento delle applicazioni utente

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| I browser Web non elaborano dati Java da Internet. | Vedi Esempio tecnico: User Application Hardening (sito web ACSC) | Non applicabile | Non applicabile |
| I browser Web non elaborano gli annunci pubblicitari Web da Internet. | | | |
| Internet Explorer 11è disabilitato o rimosso. | | | |
| Microsoft Officenon può creare processi secondari. | | | |
| Microsoft Officenon può creare contenuti eseguibili. | | | |
| Microsoft Officenon può iniettare codice in altri processi. | | | |
| Microsoft Officeè configurato per impedire l'attivazione dei pacchetti OLE. | | | |
| Al software PDF è impedito di creare processi secondari. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Vengono implementate linee guida ACSC o del fornitore per i browser Web Microsoft Office e il software PDF. | | | |
| Le impostazioni di sicurezza del browser Web Microsoft Office e del software PDF non possono essere modificate dagli utenti. | | | |
| .NET Framework3.5 (include .NET 2.0 e 3.0) è disabilitato o rimosso. | | | |
| Windows PowerShell2.0 è disabilitato o rimosso. | | | |
| PowerShellè configurato per utilizzare la modalità Linguaggio con vincoli. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le esecuzioni di PowerShell script bloccate vengono registrate centralmente e protette da modifiche ed eliminazioni non autorizzate, monitorate per rilevare eventuali segni di compromissione e intervenute quando vengono rilevati eventi di sicurezza informatica. | | | |

## Limita i privilegi amministrativi

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le richieste di accesso privilegiato a sistemi e applicazioni vengono convalidate alla prima richiesta. | Tema 4: Gestire le identità: implementa la federazione delle identità | Richiedi agli utenti umani di effettuare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee | SEC02- BP04 Affidati a un provider di identità centralizzato<br><br>SEC03- BP01 Definisci i requisiti di accesso |
| L'accesso privilegiato a sistemi e applicazioni viene automaticamente disabilitato dopo 12 mesi, a | Tema 4: Gestire le identità: implementa la federazione delle identità | Richiedi agli utenti umani di effettuare la federazione con un provider di identità per accedere AWS | SEC02- BP04 Affidati a un provider di identità centralizzato |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| meno che non venga riconvalidato. | | utilizzando credenziali temporanee | |
| | Tema 4: Gestire le identità: Ruota le credenziali | Richiedi ai carichi di lavoro di utilizzare i ruoli IAM per accedere AWS<br><br>Automatizza l'eliminazione dei ruoli IAM non utilizzati<br><br>Ruota regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine<br><br>AWS Summit ANZ 2023: il tuo percorso verso le credenziali temporanee nel cloud (video) YouTube | SEC02- BP05 Controlla e ruota periodicamente le credenziali |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| L'accesso privilegiato a sistemi e applicazioni viene disattivato automaticamente dopo 45 giorni di inattività. | Tema 4: Gestire le identità: implementa la federazione delle identità<br><br>Tema 4: Gestire le identità: Ruota le credenziali | Richiedi agli utenti umani di unirsi a un provider di identità per accedere AWS utilizzando credenziali temporanee<br><br>Richiedi ai carichi di lavoro di utilizzare i ruoli IAM per accedere AWS<br><br>Automatizza l'eliminazione dei ruoli IAM non utilizzati<br><br>Ruota regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine<br><br>AWS Summit ANZ 2023: il tuo percorso verso le credenziali temporanee nel cloud (video) YouTube | SEC02- BP04 Affidati a un provider di identità centralizzato<br><br>SEC02- BP05 Controlla e ruota periodicamente le credenziali |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| L'accesso privilegiato ai sistemi e alle applicazioni è limitato solo a ciò che è necessario agli utenti e ai servizi per svolgere i propri compiti. | Tema 4: Gestire le identità: Applica le autorizzazioni con privilegi minimi | Proteggi le credenziali dell'utente root e non utilizzarle per le attività quotidiane<br><br>Utilizza IAM Access Analyzer per generare politiche con privilegi minimi basate sull'attività di accesso<br><br>Verifica l'accesso pubblico e tra account alle risorse con IAM Access Analyzer<br><br>Utilizza IAM Access Analyzer per convalidare le tue policy IAM per autorizzazioni sicure e funzionali<br><br>Stabilisci barriere di autorizzazione su più account<br><br>Utilizza i limiti delle autorizzazioni per impostare le autorizzazioni massime che una politica basata sull'identità può concedere | SEC01- Proprietà e utente root dell'account BP02 sicuri<br><br>SEC03- BP02 Concedi l'accesso con il minimo privilegio |

| Controllo Essential Eight | Guida all'imple mentazione | AWS risorse | AWS Guida Well-Arch itected |
|---|---|---|---|
| | | Utilizza le condizion i nelle policy IAM per limitare ulteriormente l'accesso<br><br>Esamina e rimuovi regolarmente utenti, ruoli, autorizzazioni, politiche e credenziali non utilizzati<br><br>Inizia con le politiche AWS gestite e passa alle autorizzazioni con privilegi minimi<br><br>Utilizza la funzional ità dei set di autorizza zioni in IAM Identity Center | |
| Agli account privilegi ati viene impedito l'accesso a Internet, alla posta elettronica e ai servizi web. | Vedi Esempio tecnico: limitazione dei privilegi amministrativi (sito web ACSC) | Prendi in considera zione l'impleme ntazione di un SCP che impedisca a qualsiasi VPC che non dispone già di accesso a Internet di accedervi | Non applicabile |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Gli utenti privilegiati utilizzano ambienti operativi separati, privilegiati e non privilegiati. | Tema 5: Stabilire un perimetro di dati | Stabilisci un perimetro di dati. Prendi in considerazione l'implementazione di perimetri di dati tra ambienti con diverse classific azioni dei dati, ad esempio `OFFICIAL: SENSITIVE` o`PROTECTED` , o diversi livelli di rischio, come sviluppo, test o produzione. | SEC06- BP03 Ridurre la gestione manuale e l'accesso interattivo |
| Gli ambienti operativi privilegiati non sono virtualizzati all'interno di ambienti operativi non privilegiati. | | | |
| Gli account non privilegiati non possono accedere ad ambienti operativi privilegiati. | | | |
| Gli account privilegiati (esclusi gli account di amministratore locale) non possono accedere ad ambienti operativi non privilegiati. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Just-in-time l'amministrazione viene utilizzata per amministrare sistemi e applicazioni. | Tema 4: Gestire le identità: implementa la federazione delle identità | Richiedi agli utenti umani di effettuare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee<br><br>Implementa un accesso temporaneo o elevato ai tuoi AWS ambienti (AWS post sul blog) | SEC02- BP04 Affidati a un provider di identità centralizzato |
| Le attività amministrative vengono condotte tramite jump server. | Tema 1: Utilizzare i servizi gestiti<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Utilizza l'automazione anziché i processi manuali | Utilizza Session Manager o Run Command anziché l'accesso diretto SSH o RDP | SEC01- BP05 Ridurre l'ambito di gestione della sicurezza<br><br>SEC06- BP03 Ridurre la gestione manuale e l'accesso interattivo |
| Le credenziali per gli account degli amministratori locali e gli account di servizio sono uniche, imprevedibili e gestite. | Vedi Esempio tecnico: Limita i privilegi amministrativi (sito web ACSC) | Non applicabile | Non applicabile |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
| --- | --- | --- | --- |
| Windows Defender Credential Guarde Windows Defender Remote Credential Guard sono abilitati. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| L'uso dell'accesso privilegiato viene registrato centralmente e protetto da modifiche ed eliminazioni non autorizzate, monitorato per rilevare eventuali segni di compromissione e intervento quando vengono rilevati eventi di sicurezza informatica. | Tema 7: Centralizzare la registrazione e il monitoraggio: Abilita la registrazione<br><br>Tema 7: Centralizzare la registrazione e il monitoraggio: Centralizza i log | Usa CloudWatch Agent per pubblicare i log a livello di sistema operativo nei registri CloudWatch<br><br>Abilita per la tua organizzazione CloudTrail<br><br>Centralizza CloudWatch i log in un account per il controllo e l'analisi (post sul blog)AWS<br><br>Gestione centralizzata di Amazon Inspector<br><br>Gestione centralizzata del Security Hub CSPM<br><br>Crea un aggregatore a livello di organizzazione in (post del blog) AWS ConfigAWS<br><br>Centralizza la gestione di GuardDuty<br><br>Prendi in considerazione l'utilizzo di Amazon Security Lake | SEC04- BP01 Configura la registrazione dei servizi e delle applicazioni<br><br>SEC04- BP02 Acquisisci registri, risultati e metriche in posizioni standardizzate |
| Le modifiche agli account e ai gruppi privilegiati vengono registrate centralmente e protette da modifiche ed eliminazioni non autorizzate, monitorate per rilevare eventuali segni di compromissione e intervento quando vengono rilevati eventi di sicurezza informatica. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| | | Ricevi CloudTrail log da più account<br><br>Invia i registri a un account di archiviazione dei registri | |

## Patch i sistemi operativi

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le patch, gli aggiornamenti o le mitigazioni dei fornitori per le vulnerabilità di sicurezza nei sistemi operativi dei servizi connessi a Internet vengono applicati entro due settimane dal rilascio o entro 48 ore se esiste un exploit. | Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementazione di AMI e pipeline di creazione di container | Usa EC2 Image Builder e integra:<br>• AWS Systems Manager Agente (agente SSM)<br>• Strumenti di sicurezza per il controllo delle applicazioni, come Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) () o OpenSCAP GitHub<br>• CloudWatch Agente Amazon | SEC01- BP05 Riduci l'ambito della gestione della sicurezza<br><br>SEC06- BP01 Eseguire la gestione delle vulnerabilità<br><br>SEC06- BP03 Ridurre la gestione manuale e l'accesso interattivo |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| | | Condividi AMIs con l'intera organizzazione<br><br>Assicurati che i team addetti all'applicazione stiano facendo riferimento alle ultime novità AMIs<br><br>Usa la tua pipeline AMI per la gestione delle patch | |
| | Tema 1: Utilizzare i servizi gestiti: Abilita l'applicazione di patch<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Automatizza l'applicazione delle patch | Abilita Patch Manager in tutti gli account della tua organizzazione AWS | SEC06- BP01 Esegui la gestione delle vulnerabilità<br><br>SEC06- BP05 Automatizza la protezione dell'elaborazione |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le patch, gli aggiornamenti o le mitigazioni dei fornitori per le vulnerabilità di sicurezza nei sistemi operativi di workstation, server e dispositivi di rete vengono applicati entro due settimane dal rilascio o entro 48 ore se esiste un exploit. | Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementazione di AMI e pipeline di creazione di container | Usa EC2 Image Builder e integra:<br>• AWS Systems Manager Agente (agente SSM)<br>• Strumenti di sicurezza per il controllo delle applicazioni, come Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) () o OpenSCAP GitHub<br>• CloudWatch Agente Amazon<br><br>Condividi AMIs con l'intera organizzazione<br><br>Assicurati che i team addetti all'applicazione stiano facendo riferimento alle ultime novità AMIs<br><br>Usa la tua pipeline AMI per la gestione delle patch | SEC01- BP05 Riduci l'ambito della gestione della sicurezza<br><br>SEC06- BP01 Eseguire la gestione delle vulnerabilità<br><br>SEC06- BP02 Fornisci dati di calcolo a partire da immagini protette |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| | Tema 1: Utilizzare i servizi gestiti: Abilita l'applicazione di patch<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Automatizza l'applicazione delle patch | Abilita Patch Manager in tutti gli account della tua organizzazione AWS | SEC06- BP01 Esegui la gestione delle vulnerabilità<br><br>SEC06- BP05 Automatizza la protezione dell'elaborazione |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Uno scanner di vulnerabilità viene utilizzato almeno quotidianamente per identificare le patch o gli aggiornamenti mancanti per le vulnerabilità di sicurezza nei sistemi operativi dei servizi connessi a Internet. | Tema 1: Utilizzare i servizi gestiti: Scansione per individuare eventuali vulnerabilità<br><br>Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementa la scansione delle vulnerabilità<br><br>Tema 3: Gestisci l'infrastruttura mutabile con l'automazione: Implementazione della scansione delle vulnerabilità | Abilita Amazon Inspector in tutti gli account della tua organizzazione<br><br>Configura la scansione avanzata per i repository Amazon ECR utilizzando Amazon Inspector<br><br>Crea un programma di gestione delle vulnerabilità per valutare e correggere i problemi di sicurezza | SEC01- BP05 Riduci l'ambito della gestione della sicurezza<br><br>SEC06- BP01 Eseguire la gestione delle vulnerabilità<br><br>SEC06- BP02 Fornisci dati di calcolo a partire da immagini protette |
| Uno scanner di vulnerabilità viene utilizzato almeno una volta alla settimana per identificare le patch o gli aggiornamenti mancanti relativi alle vulnerabilità di sicurezza nei sistemi operativi di workstation, server e dispositivi di rete. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| L'ultima versione, o la versione precedente, dei sistemi operativi viene utilizzata per workstation, server e dispositivi di rete.<br><br>I sistemi operativi che non sono più supportati dai fornitori vengono sostituiti. | Tema 2: Gestione dell'infrastruttura immutabile tramite pipeline sicure: Implementazione della scansione delle vulnerabilità | Usa EC2 Image Builder e integra:<br>• AWS Systems Manager Agente (agente SSM)<br>• Strumenti di sicurezza per il controllo delle applicazioni, come Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) () o OpenSCAP GitHub<br>• CloudWatch Agente Amazon<br><br>Condividi AMIs con l'intera organizzazione<br><br>Assicurati che i team addetti all'applicazione stiano facendo riferimento alle ultime novità AMIs<br><br>Usa la tua pipeline AMI per la gestione delle patch | SEC01- BP05 Riduci l'ambito della gestione della sicurezza<br><br>SEC06- BP01 Eseguire la gestione delle vulnerabilità<br><br>SEC06- BP02 Fornisci dati di calcolo a partire da immagini protette |

# Autenticazione a più fattori

| Controllo Essential Eight | Guida all'imple mentazione | AWS risorse | AWS Guida Well-Arch itected |
|---|---|---|---|
| L'autenticazione a più fattori viene utilizzata dagli utenti di un'organizzazione se si autenticano ai servizi di accesso a Internet dell'orga nizzazione. | Tema 4: Gestire le identità: implementa la federazione delle identità | Richiedi agli utenti umani di effettuare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee<br><br>Implementa un accesso temporane o elevato ai tuoi ambienti AWS | SEC02- BP04 Affidati a un provider di identità centralizzato |
| | Tema 4: Gestire le identità: Applica l'autenticazione a più fattori | Richiedi MFA per l'utente root<br><br>Richiedi l'autenti cazione MFA tramite AWS IAM Identity Center<br><br>Prendi in considera zione la possibilità di richiedere l'MFA per azioni API specifiche del servizio | SEC02- BP01 Utilizza meccanismi di accesso efficaci |
| L'autenticazione a più fattori viene utilizzata dagli utenti di un'organizzazione se si autenticano su servizi di terze | Vedi Implementazione dell'autenticazione a più fattori (sito web ACSC) | Non applicabile | Non applicabile |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| parti con accesso a Internet che elaborano, archiviano o comunicano i dati sensibili dell'organizzazione. | | | |
| L'autenticazione a più fattori (se disponibile) viene utilizzata dagli utenti di un'organizzazione se si autenticano su servizi di terze parti con accesso a Internet che elaborano, archiviano o comunicano i dati non sensibili dell'organizzazione. | | | |
| L'autenticazione a più fattori è abilitata per impostazione predefinita per gli utenti non aziendali (ma gli utenti possono scegliere di disattivarla) se si autenticano ai servizi di accesso a Internet di un'organizzazione. | | | |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| L'autenticazione a più fattori viene utilizzata per autenticare gli utenti privilegiati dei sistemi. | Tema 4: Gestire le identità: implementa la federazione delle identità | Richiedi agli utenti umani di effettuare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee<br><br>Implementa un accesso temporaneo o elevato ai tuoi ambienti AWS | SEC02- BP04 Affidati a un provider di identità centralizzato |
| | Tema 4: Gestire le identità: Applica l'autenticazione a più fattori | Richiedi MFA per l'utente root<br><br>Richiedi MFA tramite IAM Identity Center<br><br>Prendi in considerazione la possibilità di richiedere l'MFA per azioni API specifiche del servizio | SEC02- BP01 Utilizza meccanismi di accesso efficaci |
| L'autenticazione a più fattori viene utilizzata per autenticare gli utenti che accedono a importanti archivi di dati. | Tema 4: Gestire le identità: Applica l'autenticazione a più fattori | Prendi in considerazione la possibilità di richiedere l'MFA per azioni API specifiche del servizio | SEC02- BP01 Utilizza meccanismi di accesso efficaci |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| L'autenticazione a più fattori è resistente all'impersonificazione da parte del verificatore e utilizza: qualcosa che gli utenti hanno e qualcosa che gli utenti conoscono, oppure qualcosa che gli utenti possiedono e che viene sbloccato da qualcosa che gli utenti conoscono o sono. | Vedi Implementazione dell'autenticazione a più fattori (sito web ACSC) | Non applicabile | Non applicabile |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| Le autenticazioni a più fattori riuscite e non riuscite vengono registrate centralmente e protette da modifiche ed eliminazioni non autorizzate, monitorate per rilevare eventuali segni di compromissione e intervenute quando vengono rilevati eventi di sicurezza informatica. | Tema 7: Centralizzare la registrazione e il monitoraggio: Abilita la registrazione<br><br>Tema 7: Centralizzare la registrazione e il monitoraggio: Centralizza i log | Centralizza i CloudWatch log in un account per il controllo e l'analisi (post sul blog)AWS<br><br>Gestione centralizzata di Amazon Inspector<br><br>Gestione centralizzata del Security Hub CSPM<br><br>Crea un aggregatore a livello di organizzazione in (post del blog) AWS ConfigAWS<br><br>Centralizza la gestione di GuardDuty<br><br>Prendi in considerazione l'utilizzo di Security Lake<br><br>Ricevi CloudTrail registri da più account<br><br>Invia i registri a un account di archiviazione dei registri | SEC04- BP01 Configura la registrazione dei servizi e delle applicazioni<br><br>SEC04- BP02 Acquisisci registri, risultati e metriche in posizioni standardizzate |

# Backup regolari

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
|---|---|---|---|
| I backup di dati, software e impostazioni di configurazione importanti vengono eseguiti e conservati in modo coordinato e resiliente in conformità ai requisiti di continuità aziendale. | Tema 6: Automatizza i backup: Automatizza il backup e il ripristino dei dati | Implementare il backup dei dati su AWS<br><br>Automatizza il backup dei dati su larga scala (post AWS sul blog) | REL09- BP01 Identifica ed esegui il backup di tutti i dati di cui è necessario eseguire il backup o riproduci i dati dalle fonti<br><br>REL09- BP02 Backup sicuri e crittografati<br><br>REL09- BP03 Esegui automaticamente il backup dei dati |
| Il ripristino di sistemi, software e dati importanti dai backup viene testato in modo coordinato nell'ambito delle esercitazioni di disaster recovery. | Tema 6: Automatizza i backup: Automatizza il backup e il ripristino dei dati<br><br>Tema 6: Automatizza i backup: Implementa la governance in tutti i tuoi risultati AWS Backup | Automatizza la convalida del ripristino dei dati con AWS Backup (AWS post sul blog)<br><br>Usa AWS Backup Audit Manager per verificare la conformità delle tue AWS Backup politiche | REL09- BP04 Eseguite il ripristino periodico dei dati per verificare l'integrità e i processi di backup |
| Gli account non privilegiati e gli account privilegiati (esclusi gli amministratori di backup) non | Tema 6: Automatizza i backup: Implementa la governance in tutti i tuoi risultati AWS Backup | Le 10 migliori pratiche di sicurezza per proteggere i backup in AWS (AWS post sul blog) | SEC08- BP04 Applica il controllo degli accessi |

| Controllo Essential Eight | Guida all'implementazione | AWS risorse | AWS Guida Well-Architected |
| --- | --- | --- | --- |
| possono accedere ai backup. | | Usa AWS Backup Vault Lock per migliorare la sicurezza delle tue casseforti di backup<br><br>Usa AWS Backup Audit Manager per verificare la conformità delle tue AWS Backup politiche | |
| Agli account non privilegiati e agli account privilegiati (esclusi gli account Backup Break Glass) viene impedito di modificare o eliminare i backup. | | | |

# Note

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di AWS prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte AWS delle sue affiliate, fornitori o licenzianti. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

# Cronologia dei documenti

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

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Aggiornamenti delle migliori pratiche | Abbiamo aggiornato questa guida per riflettere le migliori pratiche più recenti nel pilastro della sicurezza del AWS Well-Architected Framework. | 6 novembre 2024 |
| Pubblicazione iniziale | — | 20 ottobre 2023 |

# AWS Glossario delle linee guida prescrittive

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

## Numeri

7 R

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

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

# A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione di aggregazione

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

# B

bot difettoso

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

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

implementazione blu/verde

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

bot

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

botnet

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

ramo

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

accesso break-glass

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

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

# C

CAF

Vedi Cloud Adoption AWS Framework.

implementazione canaria

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

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

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

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

CV

Vedi visione artificiale.

# D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

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

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

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

# E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.
- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.
- ambiente di produzione: un'istanza di un'applicazione in esecuzione a cui gli utenti finali possono accedere. In una CI/CD pipeline, l'ambiente di produzione è l'ultimo ambiente di distribuzione.

- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

epica

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

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

# F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi modello di base.

modello di fondazione (FM)

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

# G

IA generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

# H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di blocco

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

## I

IaC

Vedi l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

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

migrazione incrementale

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

# L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

# M

machine learning (ML)

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

ramo principale

Vedi filiale.

malware

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

servizi gestiti

Servizi AWS per cui AWS gestisce il livello di infrastruttura, il sistema operativo e le piattaforme e si accede agli endpoint per archiviare e recuperare i dati. Amazon Simple Storage Service

(Amazon S3) Simple Storage Service (Amazon S3) e Amazon DynamoDB sono esempi di servizi gestiti. Questi sono noti anche come servizi astratti.

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

Un approccio alla creazione di un'applicazione con componenti indipendenti che eseguono ogni processo applicativo come microservizio. Questi microservizi comunicano attraverso un'interfaccia

ben definita utilizzando sistemi leggeri. APIs Ogni microservizio in questa architettura può essere aggiornato, distribuito e dimensionato per soddisfare la richiesta di funzioni specifiche di un'applicazione. Per ulteriori informazioni, vedere Implementazione dei microservizi su. AWS

Programma di accelerazione della migrazione (MAP)

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

migrazione su larga scala

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

fabbrica di migrazione

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

# O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

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

gestione del cambiamento organizzativo (OCM)

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

Vedi la revisione della prontezza operativa.

NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

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

# P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

Un modello che consente comunicazioni asincrone tra microservizi per migliorare la scalabilità e la reattività. Ad esempio, in un MES basato su microservizi, un microservizio può pubblicare

messaggi di eventi su un canale a cui altri microservizi possono abbonarsi. Il sistema può aggiungere nuovi microservizi senza modificare il servizio di pubblicazione.

# Q

Piano di query

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

regressione del piano di query

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

# R

Matrice RACI

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

RAG

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Region

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

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

La capacità di un'applicazione di resistere alle interruzioni o di ripristinarle. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud AWSPer ulteriori informazioni, vedere Cloud AWS Resilience.

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi obiettivo del punto di ripristino.

VERSO

Vedi obiettivo del tempo di ripristino.

runbook

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

# S

SAML 2.0

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

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

In Gestione dei segreti AWS, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi

metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, consulta Cosa c'è in un segreto di Secrets Manager? nella documentazione di Secrets Manager.

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

Una politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni

che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta le politiche di controllo del servizio nella AWS Organizations documentazione.

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

# T

tag

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

variabile di destinazione

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

elenco di attività

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

ambiente di test

Vedi ambiente.

training

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

Transit Gateway

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

# U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

# V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

# W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

# Z

exploit zero-day

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

vulnerabilità zero-day

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

prompt zero-shot

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

applicazione zombie

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

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