AWS Startup Security Baseline (SSB)AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: AWS Startup Security Baseline (SSB)AWS

Table of Contents

AWS Startup Security Baseline (AWS SSB)

Jay Michael, Amazon Web Services (AWS)

Maggio 2023 (cronologia dei documenti)

AWS Startup Security Baseline (SSB) è un insieme di controlli che crea una base minima su cui le aziende possono costruire in modo sicuro su AWS senza diminuire la loro agilità. Questi controlli costituiscono la base del livello di sicurezza e si concentrano sulla protezione delle credenziali, sull'abilitazione della registrazione e della visibilità, sulla gestione delle informazioni di contatto e sull'implementazione dei limiti dei dati di base.

I controlli in questa guida sono progettati pensando alle prime startup, per mitigare i rischi di sicurezza più comuni senza richiedere sforzi significativi. Molte startup iniziano il loro viaggio nel Cloud AWS con un singolo Account AWS. Man mano che le organizzazioni crescono, migrano verso architetture multi-account. Le indicazioni contenute in questa guida sono progettate per architetture con account singolo, ma aiutano a configurare controlli di sicurezza che possono essere facilmente migrati o modificati durante il passaggio a un'architettura multi-account.

I controlli presenti in AWS SSB sono suddivisi in due categorie: account e carico di lavoro. I controlli dell'account aiutano a mantenere l'account AWS sicuro. Include suggerimenti per la configurazione dell'accesso, delle policy e delle autorizzazioni degli utenti e su come monitorare l'account per rilevare attività non autorizzate o potenzialmente dannose. I controlli del carico di lavoro aiutano a proteggere le risorse e il codice nel cloud, ad esempio, applicazioni, processi di backend e dati. Include suggerimenti come la crittografia e la riduzione dell'ambito di accesso.

> **Note**
>
> Alcuni dei controlli consigliati in questa guida sostituiscono i valori predefiniti impostati durante la configurazione iniziale, mentre la maggior parte configura nuove impostazioni e policy. Questo documento non deve in alcun modo essere considerato completo di tutti i controlli disponibili.

Destinatari principali

Questa guida è ideale per le startup che si trovano nelle primissime fasi di sviluppo, con personale e operazioni minimi.

Le startup o altre aziende che si trovano nelle fasi successive di attività e crescita possono comunque trarre un valore significativo dall'analisi di questi controlli rispetto alle loro pratiche attuali. Se vengono identificate delle lacune, è possibile implementare i singoli controlli descritti in questa guida e poi valutarne l'adeguatezza come soluzione a lungo termine.

> **Note**
>
> I controlli suggeriti in questa guida sono controlli di base. Le startup o altre società che operano in una fase successiva di scalabilità o sofisticazione dovrebbero eventualmente aggiungere altri controlli.

Framework di base e responsabilità in materia di sicurezza

AWS Well-Architected aiuta gli architetti del cloud a creare un'infrastruttura sicura, a elevate prestazioni, resiliente ed efficiente per applicazioni e carichi di lavoro. AWS Startup Security Baseline si allinea al pilastro della sicurezza del Framework AWS Well-Architected. Il pilastro della sicurezza descrive come sfruttare le tecnologie cloud per proteggere dati, sistemi e risorse in modo da migliorare il livello di sicurezza. Ciò consente di soddisfare i requisiti aziendali e normativi seguendo i suggerimenti di AWS attuali.

È possibile valutare la propria aderenza alle best practice di Well-Architected utilizzando AWS Well-Architected Tool nell'account AWS.

Sicurezza e conformità sono una responsabilità condivisa tra AWS e il cliente. Il modello di responsabilità condivisa viene spesso descritto affermando che AWS è responsabile della sicurezza del cloud (ovvero è responsabile della protezione dell'infrastruttura che esegue tutti i servizi offerti nel Cloud AWS) e l'utente è responsabile della sicurezza nel cloud (come stabilito dai servizi del Cloud AWS selezionati). Nel modello di responsabilità condivisa, l'implementazione dei controlli di sicurezza descritti in questo documento rientra nella responsabilità dell'utente in qualità di cliente.

Protezione dell'account

I controlli e i consigli in questa sezione aiutano a proteggere il tuo AWS account. Sottolinea l'utilizzo AWS Identity and Access Management di utenti, gruppi di utenti e ruoli (noti anche come principali) per l'accesso umano e automatico, limita l'uso dell'utente root e richiede l'autenticazione a più fattori. In questa sezione confermi di disporre delle informazioni di contatto necessarie per contattarti in merito all'attività e allo AWS stato del tuo account. Inoltre, configuri servizi di monitoraggio, come AWS Trusted Advisor Amazon e GuardDuty Budget AWS, in modo da ricevere notifiche sull'attività del tuo account e poter rispondere rapidamente se l'attività non è autorizzata o inaspettata.

Questa sezione contiene i seguenti argomenti:

ACCT.01 - Imposta i contatti a livello di account su liste di distribuzione e-mail valide

Quando configuri i contatti principali e alternativi per il tuo AWS account, utilizza una lista di distribuzione e-mail anziché l'indirizzo e-mail di una persona. L'utilizzo di una lista di distribuzione e-mail assicura che la proprietà e la raggiungibilità siano preservate man mano che i singoli membri dell'organizzazione entrano ed escono. Imposta contatti alternativi per la fatturazione, le operazioni e le notifiche di sicurezza e utilizza di conseguenza le liste di distribuzione e-mail appropriate. AWS utilizza questi indirizzi e-mail per contattarti, quindi è importante che tu mantenga l'accesso ad essi.

Per modificare il nome dell'account, la password dell'utente root o l'indirizzo e-mail dell'utente root

1. Accedi alla pagina Impostazioni dell'account nella console Gestione costi e fatturazione all'indirizzo https://console.aws.amazon.com/billing/home?#/account.
2. Nella pagina Account Settings (Impostazioni account), accanto a Account Settings (Impostazioni account), scegli Edit (Modifica).
3. Accanto al campo che desideri aggiornare, scegli Modifica.
4. Dopo aver apportato le modifiche necessarie, scegli Save changes (Salva modifiche).
5. Dopo avere apportato tutte le modifiche, scegli Done (Fine).

Per modificare le informazioni di contatto,

1. Nella pagina Impostazioni dell'account, in Informazioni di contatto, scegli Modifica.
2. Per i campi da modificare, digita le informazioni aggiornate, quindi scegli Aggiorna.

Per aggiungere, aggiornare o rimuovere contatti alternativi

1. Nella pagina Impostazioni dell'account, in Contatti alternativi, scegli Modifica.
2. Per i campi da modificare, digita le informazioni aggiornate, quindi scegli Aggiorna.

ACCT.02 - Limita l'uso dell'utente root

L'utente root viene creato al momento della registrazione di un AWS account e dispone di privilegi e autorizzazioni di piena proprietà sull'account che non possono essere modificati. Usa l'utente root solo per le attività specifiche che lo richiedono. Per ulteriori informazioni, consulta Attività che richiedono credenziali utente root (AWS Account Management). Esegui tutte le altre azioni nel tuo account utilizzando altri tipi di identità IAM, ad esempio utenti federati con ruoli IAM. Per ulteriori informazioni, consulta Credenziali di sicurezza AWS (documentazione di IAM).

Per limitare l'uso dell'utente root

1. Richiedi l'autenticazione a più fattori (MFA) per l'utente root come descritto in ACCT.05 - Richiedi l'autenticazione a più fattori (MFA) per l'accesso.
2. Crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane. Per ulteriori informazioni sulla configurazione dell'accesso utente, consulta ACCT.03 - Configura l'accesso alla console per ogni utente.

ACCT.03 - Configura l'accesso alla console per ogni utente

Come procedura ottimale, AWS consiglia di utilizzare credenziali temporanee per concedere l'accesso a Account AWS risorse e risorse. Le credenziali di sicurezza provvisorie hanno una durata limitata, perciò non è necessario ruotarle o revocarle in modo esplicito quando non sono più necessarie. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie (documentazione di IAM).

Per gli utenti umani, AWS consiglia di utilizzare identità federate di un provider di identità centralizzato (IdP), come AWS IAM Identity Center Okta, Active Directory o Ping Identity. La federazione degli utenti consente di definire le identità in un'unica posizione centrale e gli utenti possono autenticarsi in modo sicuro su più applicazioni e siti Web, anche AWS utilizzando un solo set di credenziali. Per ulteriori informazioni, consulta Identity Federation in AWS e IAM Identity Center (sito Web).AWS

> **Note**
>
> La federazione delle identità può complicare la transizione da un'architettura a singolo account a un'architettura multi-account. È normale che le startup ritardino l'implementazione della federazione delle identità fino a quando non stabiliscono un'architettura multi-account gestita in AWS Organizations.

Per configurare la federazione delle identità

1. Se utilizzi IAM Identity Center, consulta Nozioni di base (documentazione di IAM Identity Center).

   Se utilizzi un IdP esterno o di terze parti, consulta Creazione di provider di identità IAM (documentazione di IAM).
2. Assicurati che il tuo IdP applichi l'autenticazione a più fattori (MFA).
3. Applica le autorizzazioni in base a ACCT.04 - Assegna autorizzazioni.

Per le startup che non sono preparate a configurare la federazione delle identità, puoi creare utenti direttamente in IAM. Questa non è una best practice di sicurezza consigliata in quanto si tratta di credenziali a lungo termine che non scadono mai. Tuttavia, questa è una pratica comune per le startup nelle prime fasi operative per evitare difficoltà nel passaggio a un'architettura multi-account quando sono pronte dal punto di vista operativo.

Di base, puoi creare un utente IAM per ogni persona che deve accedere a AWS Management Console. Se configuri utenti IAM, non condividere le credenziali tra gli utenti e ruota regolarmente le credenziali a lungo termine.

> **Warning**
>
> Gli utenti IAM dispongono di credenziali a lungo termine, il che rappresenta un rischio per la sicurezza. Per contribuire a mitigare questo rischio, ti consigliamo di fornire a questi utenti solo le autorizzazioni necessarie per eseguire l'attività e di rimuoverli quando non sono più necessari.

Per creare un utente IAM

1. Crea utenti IAM (documentazione di IAM).
2. Applica le autorizzazioni in base a ACCT.04 - Assegna autorizzazioni.

ACCT.04 - Assegna autorizzazioni

Configura le autorizzazioni utente nell'account assegnando le policy alla relativa identità IAM (gruppo utente o ruolo). È possibile personalizzare le autorizzazioni oppure allegare policy AWS gestite, che sono politiche autonome progettate per fornire autorizzazioni per AWS molti casi d'uso comuni. Se personalizzi le autorizzazioni, segui le best practice di sicurezza di concessione del privilegio minimo. Privilegio minimo è la pratica con cui viene concesso il set minimo di autorizzazioni di cui ogni utente ha bisogno per svolgere le proprie attività.

Se utilizzi identità federate, gli utenti accedono all'account assumendo un ruolo IAM tramite il provider di identità esterno. Il ruolo IAM definisce ciò che gli utenti autenticati dall'IdP della tua organizzazione possono fare. AWS A questo ruolo applichi policy personalizzate o AWS gestite per configurare le autorizzazioni.

Per assegnare le autorizzazioni per le identità federate

- Se utilizzi IAM Identity Center, consulta Utilizza policy IAM nei set di autorizzazioni (documentazione di IAM Identity Center).

  Se utilizzi un IdP esterno o di terze parti, consulta Aggiunta di autorizzazioni di identità IAM (documentazione di IAM).

Se utilizzi utenti IAM, puoi utilizzare gruppi di utenti o ruoli per gestire le autorizzazioni per più utenti IAM. Consigliamo i gruppi di utenti per le startup perché sono più facili da gestire e meno soggetti a configurazioni errate che potrebbero comportare rischi per la sicurezza del tuo account. Assegna gli utenti ai gruppi di utenti in base alle loro funzioni lavorative. Esempi di gruppi di utenti includono ingegneri che si occupano di applicazioni, dati, reti e Development Operations (DevOps). Puoi anche suddividere i tipi di utenti in gruppi di utenti più piccoli in base all'autorità decisionale, ad esempio per ingegneri senior o non senior.

Per assegnare autorizzazioni per utenti IAM

1. Crea gruppi di utenti IAM (documentazione di IAM).
2. Allega una policy AWS gestita a un gruppo di utenti IAM (documentazione IAM).

ACCT.05 - Richiedi l'autenticazione a più fattori (MFA) per l'accesso

Con MFA, gli utenti dispongono di un dispositivo che genera una risposta a una richiesta di autenticazione. Per completare la procedura di accesso, sono necessarie le credenziali dell'utente e la risposta generata dal dispositivo. Come best practice di sicurezza, abilita l'MFA per Account AWS l'accesso, in particolare per le credenziali a lungo termine come l'utente root dell'account e gli utenti IAM.

Per configurare MFA per l'utente root

1. Accedi all'indirizzo. AWS Management Console https://console.aws.amazon.com/
2. Nel lato destro della barra di navigazione, seleziona il nome dell'account, quindi scegli Le mie credenziali di sicurezza.
3. Se necessario, selezionare Continue to Security Credentials (Continua alle credenziali di sicurezza).
4. Espandere la sezione Multi-Factor Authentication (MFA) (Autenticazione a più fattori (MFA)).
5. Scegliere Activate MFA (Attiva MFA).
6. Segui le istruzioni della procedura guidata per configurare i tuoi dispositivi MFA di conseguenza. Per ulteriori informazioni, consulta Abilitazione dei dispositivi MFA per gli utenti in AWS (documentazione di IAM).

Per configurare MFA in IAM Identity Center

- Abilita MFA (documentazione di IAM Identity Center)

Per configurare MFA per il tuo utente IAM

1. Accedi alla console IAM all'indirizzo https://console.aws.amazon.com/iam utilizzando le credenziali di accesso.
2. Selezionare il nome utente in alto a destra nella barra di navigazione e selezionare My Security Credentials (Le mie credenziali di sicurezza).
3. Nella scheda Credenziali AWS IAM, nella sezione Autenticazione a più fattori, seleziona Gestione dispositivo MFA.

Per configurare MFA per altri utenti IAM

1. Accedi AWS Management Console e apri la console IAM all'indirizzohttps://console.aws.amazon.com/iam.
2. Nel pannello di navigazione, seleziona Utenti.
3. Selezionare il nome dell'utente per il quale si deve abilitare l'autorizzazione MFA e selezionare la scheda Credenziali di sicurezza.
4. Accanto ad Assigned MFA device (Dispositivo MFA assegnato), selezionare Gestione.
5. Segui le istruzioni della procedura guidata per configurare i tuoi dispositivi MFA di conseguenza. Per ulteriori informazioni, consulta Abilitazione dei dispositivi MFA per gli utenti in AWS (documentazione di IAM).

ACCT.06 - Applica una policy per password

Gli utenti accedono a AWS Management Console fornendo le credenziali di accesso e si consiglia l'autenticazione MFA. Richiedi che le password siano conformi a una policy delle password sicure per evitare che vengano scoperte tramite la forza bruta o l'ingegneria sociale.

Per ulteriori informazioni sui suggerimenti più recenti per password sicure, consulta Guida alla policy delle password sul sito Web di Center for Internet Security (CIS).

Per gli utenti IAM, puoi configurare i requisiti relativi alle password in una policy delle password IAM personalizzata. Per ulteriori informazioni, consulta Impostazione di una policy delle password per gli account (documentazione di IAM).

Per creare una policy delle password personalizzata

1. Accedi AWS Management Console e apri la console IAM all'indirizzo. https://console.aws.amazon.com/iam
2. Nel riquadro di navigazione, scegliere Account settings (Impostazioni account).
3. Nella sezione Policy delle password, scegli Cambia la policy per le password.
4. Seleziona le opzioni che desideri applicare alla policy delle password e scegli Salva modifiche.

ACCT.07: consegna i CloudTrail log a un bucket S3 protetto

Le azioni intraprese da utenti, ruoli e servizi nel tuo AWS account vengono registrate come eventi in AWS CloudTrail. CloudTrail è abilitato per impostazione predefinita e nella CloudTrail console è possibile accedere a 90 giorni di informazioni sulla cronologia degli eventi. Per visualizzare, cercare, scaricare, archiviare, analizzare e rispondere alle attività degli account nell' AWS infrastruttura, vedi Visualizzazione degli eventi con la cronologia degli CloudTrail eventi (CloudTrail documentazione).

Per conservare CloudTrail la cronologia oltre 90 giorni con dati aggiuntivi, crei un nuovo trail che invia i file di log a un bucket Amazon Simple Storage Service (Amazon S3) per tutti i tipi di eventi. Quando crei un percorso nella CloudTrail console, crei un percorso multiregionale.

Per creare un percorso che fornisca i log per tutti Regioni AWS a un bucket S3

1. Crea un percorso (documentazione)CloudTrail . Nella pagina Scegli eventi di log, esegui le operazioni seguenti:
    a. Per Attività API, scegli Lettura e Scrittura.
    b. Per gli ambienti di preproduzione, scegli Escludi eventi AWS KMS . Questo esclude tutti gli eventi AWS Key Management Service (AWS KMS) dal tuo percorso. AWS KMS leggi azioni come `EncryptDecrypt`, e `GenerateDataKey` può generare un grande volume di eventi.

        Per gli ambienti di produzione, scegli di registrare gli eventi di gestione scrittura, quindi deseleziona la casella di controllo per Escludi eventi AWS KMS . Ciò esclude gli eventi di AWS KMS lettura ad alto volume, ma registra comunque gli eventi di scrittura pertinenti,

comeDisable, Delete e. ScheduleKey Queste sono le impostazioni di AWS KMS registrazione minime consigliate per un ambiente di produzione.

2. Il nuovo trail viene visualizzato nella pagina Trails (Trail). In circa 15 minuti, CloudTrail pubblica file di registro che mostrano le chiamate API (AWS Application Programming Interface) effettuate nell'account. È possibile visualizzare i file di log nel bucket S3 specificato.

Per proteggere i bucket S3 in cui vengono archiviati i file di registro CloudTrail

1. Consulta la policy sui bucket di Amazon S3 (CloudTrail documentazione) per tutti i bucket in cui memorizzi i file di log e modificala secondo necessità per rimuovere eventuali accessi non necessari.
2. Come best practice per la sicurezza, assicurati di aggiungere manualmente una chiave di condizione `aws:SourceArn` per la policy del bucket. Per ulteriori informazioni, consulta Creare o aggiornare un bucket Amazon S3 da utilizzare per archiviare i file di log per un percorso organizzativo (CloudTrail documentazione).
3. Abilita l'eliminazione MFA (documentazione di Amazon S3).

ACCT.08 - Impedisci l'accesso pubblico ai bucket S3 privati

Per impostazione predefinita, solo l'utente root del principale IAM Account AWS e il principale IAM, se utilizzato, dispongono delle autorizzazioni di lettura e scrittura sui bucket Amazon S3 creati da tale principale. L'accesso ad altri principali IAM viene concesso utilizzando policy basate su identità e le condizioni di accesso possono essere applicate utilizzando una policy per bucket. È possibile creare policy per bucket che garantiscano l'accesso pubblico generale al bucket, un bucket pubblico.

I bucket creati a partire dal 28 aprile 2023 hanno l'opzione Blocca accesso pubblico abilitata per impostazione predefinita. Per i bucket creati prima di questa data, gli utenti potrebbero configurare erroneamente la policy e concedere involontariamente l'accesso al pubblico. È possibile evitare questa configurazione errata abilitando l'impostazione Blocca accesso pubblico per ogni bucket. Se non hai casi d'uso attuali o futuri per un bucket S3 pubblico, abilita questa impostazione a livello. Account AWS Questa impostazione impedisce le policy che consentono l'accesso pubblico.

Per impedire l'accesso pubblico ai bucket S3

- Configura le impostazioni di blocco dell'accesso pubblico per i bucket S3 (documentazione di Amazon S3).

AWS Trusted Advisor genera un risultato giallo per i bucket S3 che consentono l'accesso pubblico in modalità elenco o lettura e genera un risultato rosso per i bucket che consentono caricamenti o eliminazioni pubblici. Come linea di base, segui il controllo ACCT.12 - Monitora e risolvi i problemi ad alto rischio utilizzando Trusted Advisor per identificare e correggere i bucket non configurati correttamente. I bucket S3 accessibili al pubblico sono indicati anche nella console Amazon S3.

ACCT.09 - Elimina VPC, sottoreti e gruppi di sicurezza non utilizzati

Per ridurre la possibilità di problemi di sicurezza, elimina o disattiva tutte le risorse che non vengono utilizzate. In un nuovo AWS account, per impostazione predefinita viene creato automaticamente un cloud privato virtuale (VPC) in ogni account Regione AWS, che consente di assegnare indirizzi IP pubblici nelle sottoreti pubbliche. Tuttavia, se questi VPC non sono necessari, ciò comporta il rischio di esposizione involontaria delle risorse.

Se non sono in uso, elimina i VPC predefiniti in tutte le regioni, non solo quelli nelle regioni in cui potresti distribuire carichi di lavoro. L'eliminazione di un VPC comporta anche l'eliminazione dei relativi componenti, come sottoreti e gruppi di sicurezza.

> **Note**
>
> Puoi visualizzare tutte le regioni e i VPC nella console Amazon EC2 Global View all'indirizzo https://console.aws.amazon.com/ec2globalview/home. Per ulteriori informazioni, consulta la pagina Elenca e filtra le risorse in tutte le regioni utilizzando Amazon EC2 Global View (documentazione di Amazon EC2).

Per eliminare i VPC predefiniti non utilizzati

1. Elimina il VPC (documentazione di Amazon VPC).
2. Ripeti per i VPC nelle altre regioni, se necessario.

ACCT.10 — Configura per monitorare le tue spese Budget AWS

Budget AWS abilita il monitoraggio dei costi e dell'utilizzo mensili con notifiche quando si prevede che i costi superino le soglie prefissate. Le notifiche sui costi previsti possono fornire un'indicazione di attività impreviste, fornendo una difesa aggiuntiva oltre ad altri sistemi di monitoraggio, come AWS

Trusted Advisor Amazon. GuardDuty Anche il monitoraggio e la comprensione AWS dei costi fanno parte di una buona igiene operativa.

Per impostare un budget in Budget AWS

- Creare un budget di costi (Budget AWS documentazione).

ACCT.11 — Abilita e rispondi alle notifiche GuardDuty

Amazon GuardDuty è un servizio di rilevamento delle minacce che monitora continuamente i comportamenti dannosi o non autorizzati per proteggere AWS account, carichi di lavoro e dati. Quando rileva attività impreviste e potenzialmente dannose, GuardDuty fornisce risultati di sicurezza dettagliati per visibilità e correzione. GuardDuty è in grado di rilevare minacce come l'attività di mining di criptovalute, l'accesso da client e relè Tor, comportamenti imprevisti e credenziali IAM compromesse. Abilita GuardDuty e rispondi ai risultati per bloccare comportamenti potenzialmente dannosi o non autorizzati nel tuo ambiente. AWS Per ulteriori informazioni sui risultati in GuardDuty, vedere Finding types (GuardDuty documentazione).

Puoi utilizzare Amazon CloudWatch Events per configurare notifiche automatiche quando si GuardDuty crea un risultato o la ricerca viene modificata. Innanzitutto, puoi creare un argomento Amazon Simple Notification Service (Amazon SNS) e aggiungere endpoint, o indirizzi e-mail, all'argomento. Quindi, configuri un CloudWatch evento per GuardDuty i risultati e la regola dell'evento notifica gli endpoint nell'argomento Amazon SNS.

Attivazione e notifiche GuardDuty GuardDuty

1. Abilita Amazon GuardDuty (GuardDuty documentazione).
2. Crea una regola CloudWatch Events per notificarti i GuardDuty risultati (GuardDutydocumentazione).

ACCT.12 - Monitora e risolvi i problemi ad alto rischio utilizzando Trusted Advisor

AWS Trusted Advisor analizza passivamente l' AWS infrastruttura alla ricerca di problemi ad alto rischio o ad alto impatto relativi a sicurezza, prestazioni, costi e affidabilità. Fornisce informazioni dettagliate sulle risorse interessate e suggerimenti per la correzione. Per un

elenco completo dei controlli e delle descrizioni, consulta AWS Trusted Advisor check reference (documentazione).Trusted Advisor

Esamina Trusted Advisor i risultati su base ricorrente e correggi i problemi se necessario. Se disponi dei piani AWS Business Support o Enterprise Support, puoi iscriverti a un'e-mail settimanale con i risultati. Per ulteriori informazioni, consulta Configura le preferenze di notifica (documentazione di AWS Support).

Per visualizzare i problemi in Trusted Advisor

- Esamina ogni categoria di controllo in base alle istruzioni in Visualizza le categorie di controllo (AWS Support documentazione). Suggeriamo di rivedere almeno i problemi di tipo azione consigliata, che sono visualizzati in rosso.

Protezione dei carichi di lavoro

I controlli e i suggerimenti in questa sezione consentono di proteggere i carichi di lavoro in esecuzione in AWS, mentre vengono creati. Sottolineano le pratiche sicure per la gestione dei segreti delle applicazioni e dell'ambito di accesso, la riduzione al minimo dei percorsi di accesso alle risorse private e l'utilizzo della crittografia per proteggere i dati in transito e inattivi.

Questa sezione contiene gli argomenti seguenti:

WKLD.01 - Usa i ruoli IAM per le autorizzazioni dell'ambiente di calcolo

In AWS Identity and Access Management (IAM), un ruolo rappresenta un set di autorizzazioni che possono essere concesse da una persona o da un servizio per un periodo di tempo configurabile. L'utilizzo dei ruoli elimina la necessità di archiviare o gestire le credenziali a lungo termine, riducendo in modo significativo la possibilità di un uso non intenzionale. Assegna un ruolo IAM direttamente

alle istanze di Amazon Elastic Compute Cloud (Amazon EC2), ad attività e servizi AWS Fargate, a funzioni AWS Lambda e ad altri servizi di calcolo AWS ogni volta che sono supportati. Le applicazioni che utilizzano un SDK AWS e vengono eseguite in questi ambienti di calcolo utilizzano automaticamente le credenziali del ruolo IAM per l'autenticazione.

L'approccio e le istruzioni per l'utilizzo dei ruoli IAM per ciascun servizio sono disponibili nella Documentazione di AWS relativa al servizio. Ad esempio, consulta quanto segue:

- Ruoli IAM per Amazon EC2 (documentazione di Amazon EC2)
- Ruoli IAM per le attività (documentazione di Amazon Elastic Container Service)
- Ruolo di esecuzione Lambda (documentazione di Lambda)

WKLD.02 - Limita l'ambito di utilizzo delle credenziali con le autorizzazioni delle policy basate sulle risorse

Le policy sono oggetti che possono definire le autorizzazioni o specificare le condizioni di accesso. Sono disponibili due tipi principali di policy:

- Le policy basate sull'identità sono collegate ai principali e definiscono quali sono le autorizzazioni del principale nell'ambiente AWS.
- Le policy basate sulle risorse sono collegate a una risorsa, ad esempio un bucket Amazon Simple Storage Service (Amazon S3) o un endpoint di cloud privato virtuale (VPC). Queste policy specificano a quali principali è consentito l'accesso, le azioni supportate e qualsiasi altra condizione che deve essere soddisfatta.

Per poter accedere ed eseguire un'azione su una risorsa, un principale deve disporre dell'autorizzazione concessa nella policy basata sulle identità e soddisfare le condizioni della policy basata sulle risorse. Per ulteriori informazioni, consulta Policy basate sulle identità e policy basate sulle risorse (documentazione di IAM).

Le condizioni consigliate per le policy basate sulle risorse includono:

- Limita l'accesso solo ai principali di un'organizzazione specificata (definita in AWS Organizations) utilizzando la condizione `aws:PrincipalOrgID`.
- Limita l'accesso al traffico proveniente da un VPC o da un endpoint VPC specifico utilizzando rispettivamente la condizione `aws:SourceVpc` o `aws:SourceVpce`.

- Consenti o nega il traffico in base all'indirizzo IP di origine utilizzando una condizione `aws:SourceIp`.

Di seguito è riportato un esempio di policy basata sulle risorse che utilizza la condizione `aws:PrincipalOrgID` per consentire solo ai principali nell'organizzazione **<o-xxxxxxxxxxx>** di accedere al bucket S3 **<bucket-name>**:

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
     }
   ]
}
```

WKLD.03 - Usa segreti effimeri o un servizio di gestione dei segreti

I segreti delle applicazioni sono costituiti principalmente da credenziali, come coppie di chiavi, token di accesso, certificati digitali e credenziali di accesso. L'applicazione utilizza questi segreti per accedere ad altri servizi da cui dipende, come un database. Per proteggere questi segreti, consigliamo che siano effimeri (generati al momento della richiesta e di breve durata, come per i ruoli IAM) o recuperati da un servizio di gestione dei segreti. Ciò impedisce l'esposizione accidentale attraverso meccanismi meno sicuri, come la persistenza in file di configurazione statici. Questo semplifica anche la promozione del codice dell'applicazione dagli ambienti di sviluppo a quelli di produzione.

Per un servizio di gestione dei segreti, consigliamo di utilizzare una combinazione di Parameter Store, una funzionalità di AWS Systems Manager e AWS Secrets Manager:

- Utilizza Parameter Store per gestire segreti e altri parametri che sono coppie chiave-valore individuali, basate su stringhe, di lunghezza complessiva breve e a cui si accede frequentemente.

Utilizza una chiave AWS Key Management Service (AWS KMS) per crittografare il segreto. La memorizzazione dei parametri nel livello standard di Parameter Store è gratuita. Per ulteriori informazioni sui livelli dei parametri, consulta Gestione dei livelli dei parametri (documentazione di Systems Manager).

- Utilizza Secrets Manager per archiviare segreti in formato documento (come più coppie chiave-valore correlate), che hanno dimensioni superiori a 4 KB (come i certificati digitali) o che trarrebbero vantaggio dalla rotazione automatizzata.

È possibile utilizzare le API di Parameter Store per recuperare i segreti archiviati in Secrets Manager. Ciò consente di standardizzare il codice dell'applicazione quando si utilizza una combinazione di entrambi i servizi.

Per gestire i segreti in Parameter Store

1. Crea una chiave AWS KMS simmetrica (documentazione di AWS KMS).
2. Crea un parametro SecureString (documentazione di Systems Manager). I segreti in Parameter Store utilizzano il tipo di dati `SecureString`.
3. Nell'applicazione, recupera un parametro da Parameter Store utilizzando l'SDK AWS per il tuo linguaggio di programmazione. Per un esempio in Java, vedi GetParameter.java (AWS Code Sample Catalog).

Per gestire i segreti in Secrets Manager

1. Crea un segreto (documentazione di Secrets Manager).
2. Recupera segreti da AWS Secrets Manager in codice (documentazione di Secrets Manager).

   È importante leggere Utilizza librerie di memorizzazione nella cache lato client AWS Secrets Manager per migliorare la disponibilità e la latenza dell'utilizzo dei segreti (post sul blog di AWS). L'utilizzo di SDK lato client, che dispongono già di best practice implementate, dovrebbe accelerare e semplificare l'uso e l'integrazione di Secrets Manager.

WKLD.04 - Impedisci che i segreti delle applicazioni vengano rivelati

Durante lo sviluppo locale, i segreti delle applicazioni possono essere archiviati in file di configurazione o di codice locali e archiviati accidentalmente nei repository del codice sorgente. I repository non protetti ospitati presso fornitori di servizi pubblici possono essere soggetti all'accesso non autorizzato e i segreti possono essere scoperti. Utilizza gli strumenti disponibili per impedire che i segreti vengano archiviati. Incorpora i controlli dei segreti esposti come parte dei processi di revisione manuale del codice.

Alcuni strumenti comuni che possono impedire che i segreti delle applicazioni vengano archiviati nei repository del codice sorgente sono:

- Gitleaks (repository GitHub)
- Whispers (repository GitHub)
- detect-secrets (repository GitHub)
- git secrets (repository GitHub)
- TruffleHog (repository GitHub)

WKLD.05 - Rileva e correggi i segreti esposti

In WKLD.03 - Usa segreti effimeri o un servizio di gestione dei segreti e WKLD.04 - Impedisci che i segreti delle applicazioni vengano rivelati, hai messo in atto misure per proteggere i segreti. In questo controllo, implementi una soluzione in grado di rilevare se i segreti hanno aggirato queste misure di prevenzione e puoi porre rimedio di conseguenza.

Revisore Amazon CodeGuru rileva i segreti delle applicazioni nel codice sorgente e fornisce un meccanismo per correggere e pubblicare i segreti rilevati in Secrets Manager. Viene fornito anche il codice applicativo per recuperare il segreto da Secrets Manager. Esegui un'analisi costi-benefici per determinare se questa soluzione è adatta alla tua azienda. In alternativa, alcune delle soluzioni open source di WKLD.04 - Impedisci che i segreti delle applicazioni vengano rivelati forniscono funzionalità di rilevamento dei segreti esistenti.

Per configurare l'integrazione di CodeGuru Reviewer con Secrets Manager

- Usa CodeGuru Reviewer per identificare i segreti codificati e AWS Secrets Manager per proteggerli (post sul blog di AWS e guida dettagliata).

WKLD.06 - Usa Systems Manager anziché SSH o RDP

Le sottoreti pubbliche, che hanno un instradamento predefinito che punta a un gateway Internet, rappresentano intrinsecamente un rischio per la sicurezza maggiore rispetto alle sottoreti private, senza instradamento a Internet. È possibile eseguire istanze EC2 in sottoreti private e utilizzare la funzionalità Session Manager di AWS Systems Manager per accedere in remoto alle istanze tramite AWS Command Line Interface (AWS CLI) o AWS Management Console. È quindi possibile utilizzare la AWS CLI o la console per avviare una sessione che si connette all'istanza tramite un tunnel sicuro, evitando la necessità di gestire credenziali aggiuntive utilizzate per Secure Shell (SSH) o il protocollo desktop remoto (RDP) Windows.

Usa Session Manager invece di eseguire istanze EC2 in sottoreti pubbliche, eseguire jumpbox o eseguire host bastione.

Per configurare Session Manager

1. Assicurati che l'istanza EC2 utilizzi il sistema operativo Amazon Machine Images (AMI) più recente, come Amazon Linux 2 o Ubuntu. L'agente AWS Systems Manager (agente SSM) è preinstallato sull'AMI.
2. Assicurati che l'istanza sia connessa, tramite un gateway Internet o tramite endpoint VPC, a questi indirizzi (sostituendo **<region>** con la Regione AWS appropriata):
    a. Ec2messages.<regione>.amazonaws.com
    b. ssm.<regione>.amazonaws.com
    c. ssmmessages.<regione>.amazonaws.com
3. Collega la policy gestita AWS `AmazonSSMManagedInstanceCore` al ruolo IAM associato alle tue istanze.

Per ulteriori informazioni, consulta Configurazione di Session Manager (documentazione di Systems Manager).

Per avviare una sessione

- Avvia una sessione (documentazione di Systems Manager).

WKLD.07 - Registra gli eventi relativi ai dati per i bucket S3 con dati sensibili

Per impostazione predefinita, AWS CloudTrail acquisisce gli eventi di gestione, gli eventi che creano, modificano o eliminano risorse nel tuo account. Questi eventi di gestione non acquisiscono operazioni di lettura o scrittura su singoli oggetti nei bucket Amazon Simple Storage Service. Durante un evento di sicurezza, è importante acquisire l'accesso o l'uso non autorizzato dei dati a livello di singolo record o di oggetto. Utilizza CloudTrail per registrare gli eventi dei dati per qualsiasi bucket S3 che archivia dati sensibili o critici per l'azienda, a scopo di rilevamento e controllo.

> **Note**
>
> Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail.

Per registrare eventi di dati per i trail

1. Accedi alla AWS Management Console e apri la console CloudTrail all'indirizzo https://console.aws.amazon.com/cloudtrail/
2. Nel pannello di navigazione, scegli Trails (Percorsi) e quindi scegli il nome del percorso.
3. In Dettagli generali, scegli Modifica per modificare le seguenti impostazioni. Non puoi modificare il nome di un percorso.
    a. Per Eventi di dati, scegli Modifica.
    b. Per Data event source (Origine evento di dati), scegli S3.
    c. Per Tutti i bucket S3 attuali e futuri, deseleziona Lettura e Scrittura.
    d. In Selezione di singoli bucket, cerca un bucket in cui registrare gli eventi di dati. Puoi selezionare più bucket in questa finestra. Scegli Add bucket (Aggiungi bucket) per registrare eventi di dati per più bucket. Scegli di registrare gli eventi Read (Lettura), ad esempio `GetObject`, gli eventi Write (Scrittura), ad esempio `PutObject`, oppure entrambi.
    e. Scegli Update trail (Aggiorna percorso).

WKLD.08 - Crittografa i volumi Amazon EBS

Applica la crittografia dei volumi Amazon Elastic Block Store (Amazon EBS) come comportamento predefinito nel tuo account AWS. I volumi crittografati hanno le stesse prestazioni delle operazioni di input/output al secondo (IOPS) dei volumi non crittografati, con un effetto minimo sulla latenza. Ciò impedisce la ricostruzione dei volumi in un secondo momento per motivi di conformità o per altri motivi. Per ulteriori informazioni, consulta Best practice indispensabili per la crittografia di Amazon EBS (post sul blog di AWS).

Per crittografare i volumi Amazon EBS

- Attiva la crittografia per impostazione predefinita (documentazione di Amazon EC2).

WKLD.09 - Crittografa i database Amazon RDS

Allo stesso modo di WKLD.08 - Crittografa i volumi Amazon EBS, abilita la crittografia dei database di Amazon Relational Database Service (Amazon RDS). Questa crittografia viene eseguita a livello di volume sottostante e offre le stesse prestazioni IOPS dei volumi non crittografati, con un effetto minimo sulla latenza. Per ulteriori informazioni, consulta Panoramica della crittografia delle risorse Amazon RDS (documentazione di Amazon RDS).

Per crittografare un'istanza del database RDS

- Crittografa un'istanza del database (documentazione di Amazon RDS).

WKLD.10 - Distribuisci risorse private in sottoreti private

Distribuisci risorse che non richiedono l'accesso diretto a Internet, come istanze EC2, database, code, cache o altre infrastrutture, in una sottorete privata VPC. Le sottoreti private non hanno un instradamento dichiarato nella tabella di routing verso un gateway Internet collegato e non possono ricevere traffico Internet. Il traffico proveniente da una sottorete privata destinata a Internet deve essere sottoposto alla Network Address Translation (NAT) tramite un gateway NAT AWS gestito o un'istanza EC2 che esegue processi NAT in una sottorete pubblica. Per ulteriori informazioni sull'isolamento della rete, consulta Sicurezza dell'infrastruttura in Amazon VPC (documentazione di Amazon VPC).

Utilizza le seguenti pratiche per creare risorse e sottoreti private:

- Quando crei una sottorete privata, disabilita Assegna automaticamente un indirizzo IPv4 pubblico.
- Quando crei istanze EC2 private, disabilita Assegna automaticamente un IP pubblico. Ciò impedisce l'assegnazione di un IP pubblico se l'istanza viene distribuita involontariamente in una sottorete pubblica tramite una configurazione errata.

Se necessario, specifica la sottorete di una risorsa come parte della sua configurazione. È possibile distribuire un VPC che segue le best practice utilizzando l'avvio rapido dell'architettura VPC modulare e scalabile (Avvio rapido di AWS).

WKLD.11 - Limita l'accesso alla rete utilizzando gruppi di sicurezza

Utilizza i gruppi di sicurezza per controllare il traffico verso le istanze EC2, i database RDS e altre risorse supportate. I gruppi di sicurezza agiscono come un firewall virtuale che può essere applicato a qualsiasi gruppo di risorse correlate per definire in modo coerente le regole che consentono il traffico in entrata e in uscita. Oltre alle regole basate su indirizzi IP e porte, i gruppi di sicurezza supportano regole per consentire il traffico proveniente da risorse associate ad altri gruppi di sicurezza. Ad esempio, un gruppo di sicurezza del database può avere regole per consentire solo il traffico proveniente da un gruppo di sicurezza del server delle applicazioni.

Per impostazione predefinita, i gruppi di sicurezza consentono tutto il traffico in uscita ma non il traffico in entrata. La regola del traffico in uscita può essere rimossa oppure è possibile configurare regole aggiuntive per limitare il traffico in uscita e consentire il traffico in entrata. Se il gruppo di sicurezza è privo di regole in uscita, non viene autorizzato alcun traffico in uscita proveniente dalla tua istanza. Per ulteriori informazioni consulta Controllo del traffico verso le risorse tramite gruppi di sicurezza (documentazione di Amazon VPC).

Nell'esempio seguente, ci sono tre gruppi di sicurezza che controllano il traffico da un Application Load Balancer alle istanze EC2 che si connettono a un database Amazon RDS per MySQL.

Gruppo di sicurezza	Regole in entrata	Regole in uscita
Gruppo di sicurezza per Application Load Balancer	Descrizione: consente il traffico HTTPS da qualsiasi luogo Tipo: HTTPS	Descrizione: consente tutto il traffico verso qualsiasi luogo Tipo: tutto il traffico Destinazione: Anywhere-IPv4 (0,0.0.0/0)

Gruppo di sicurezza	Regole in entrata	Regole in uscita
	Origine: Anywhere-IPv4 (0.0.0.0/0)	
Gruppo di sicurezza dell'istanza EC2	Descrizione: consente il traffico HTTP dall'Application Load Balancer Type (Tipo): HTTP Origine: gruppo di sicurezza per l'Application Load Balancer	Descrizione: consente tutto il traffico verso qualsiasi luogo Tipo: tutto il traffico Destinazione: Anywhere-IPv4 (0,0.0.0/0)
Gruppo di sicurezza del database RDS	Descrizione: consente il traffico MySQL dall'istanza EC2 Tipo: MySQL Origine: gruppo di sicurezza dell'istanza EC2	Nessuna regola in uscita

WKLD.12 - Utilizza gli endpoint VPC per accedere ai servizi supportati

Nei VPC, le risorse che devono accedere ad AWS o ad altri servizi esterni richiedono un instradamento verso Internet (`0.0.0.0/0`) o verso l'indirizzo IP pubblico del servizio di destinazione. Utilizza gli endpoint VPC per abilitare un instradamento IP privato dal tuo VPC ad AWS o ad altri servizi supportati, evitando la necessità di utilizzare un gateway Internet, un dispositivo NAT, una connessione di rete privata virtuale (VPN) o una connessione AWS Direct Connect.

Gli endpoint VPC supportano il collegamento di policy e gruppi di sicurezza per controllare ulteriormente l'accesso a un servizio. Ad esempio, puoi scrivere una policy di endpoint VPC per Amazon DynamoDB per consentire solo azioni a livello di elemento e impedire azioni a livello di tabella per tutte le risorse nel VPC, indipendentemente dalla policy di autorizzazione. Puoi anche scrivere una policy sui bucket S3 per consentire solo le richieste provenienti da uno specifico

endpoint VPC, negando tutti gli altri accessi esterni. Un endpoint VPC può anche avere una regola del gruppo di sicurezza che, ad esempio, limita l'accesso solo alle istanze EC2 associate a un gruppo di sicurezza specifico dell'applicazione, come il livello di logica aziendale di un'applicazione Web.

Esistono diversi tipi di endpoint VPC. È possibile accedere alla maggior parte dei servizi utilizzando un endpoint di interfaccia VPC. Per l'accesso a DynamoDB viene utilizzato un endpoint di gateway. Amazon S3 supporta sia gli endpoint di gateway che gli endpoint di interfaccia. Gli endpoint di gateway sono consigliati per i carichi di lavoro contenuti in un unico account e regione AWS e sono disponibili senza costi aggiuntivi. Gli endpoint di interfaccia sono consigliati se è necessario un accesso più estensibile, ad esempio a un bucket S3 da altri VPC, da reti on-premise o da altre Regioni AWS. Gli endpoint di interfaccia prevedono un costo di operatività orario e un costo di elaborazione dati per GB, entrambi inferiori ai rispettivi costi per l'invio dei dati a `0.0.0.0/0` attraverso un gateway NAT AWS.

Per ulteriori informazioni sull'utilizzo di endpoint VPC, consulta le seguenti risorse:

- Per ulteriori informazioni sulla selezione di endpoint di gateway ed endpoint di interfaccia per Amazon S3, consulta Scelta della strategia di endpoint VPC per Amazon S3 (post sul blog di AWS).
- Crea un endpoint di interfaccia (documentazione di Amazon VPC).
- Crea un endpoint di gateway (documentazione di Amazon VPC).
- Ad esempio, per le policy di bucket S3 che limitano l'accesso a un VPC o a un endpoint VPC specifico, consulta Limitazione dell'accesso a un VPC specifico (documentazione di Amazon S3).
- Ad esempio, per le policy di endpoint DynamoDB che limitano le azioni, consulta Policy di endpoint per DynamoDB (documentazione di Amazon VPC).

WKLD.13 - Richiedi HTTPS per tutti gli endpoint Web pubblici

Richiedi HTTPS per fornire ulteriore credibilità ai tuoi endpoint Web, consentire agli endpoint di utilizzare certificati per dimostrare la propria identità e confermare che tutto il traffico tra l'endpoint e i client connessi sia crittografato. Per i siti Web pubblici, ciò offre l'ulteriore vantaggio di un posizionamento più elevato nei motori di ricerca.

Molti servizi AWS forniscono endpoint Web pubblici per le risorse, ad esempio AWS Elastic Beanstalk, Amazon CloudFront, Gateway Amazon API, Elastic Load Balancing e AWS Amplify. Per istruzioni su come richiedere HTTPS per ciascuno di questi servizi, consulta quanto segue:

- Elastic Beanstalk (documentazione di Elastic Beanstalk)
- CloudFront (documentazione di CloudFront)
- Application Load Balancer (AWS Knowledge Center)
- Classic Load Balancer (AWS Knowledge Center)
- Amplify (documentazione di Amplify)

I siti Web statici ospitati su Amazon S3 non supportano HTTPS. Per richiedere HTTPS per questi siti Web, puoi utilizzare CloudFront. Non è richiesto l'accesso pubblico ai bucket S3 che forniscono contenuti tramite CloudFront.

Per utilizzare CloudFront per gestire un sito Web statico ospitato su Amazon S3

1. Usa CloudFront per gestire un sito Web statico ospitato su Amazon S3 (AWS Knowledge Center).
2. Se stai configurando l'accesso a un bucket S3 pubblico, richiedi HTTPS tra i visualizzatori e CloudFront (documentazione di CloudFront).

   Se stai configurando l'accesso a un bucket S3 privato, limita l'accesso ai contenuti di Amazon S3 utilizzando un'identità di accesso di origine (documentazione di CloudFront).

Inoltre, configura gli endpoint HTTPS in modo che richiedano protocolli e cifrari moderni di Transport Layer Security (TLS), a meno che non sia necessaria la compatibilità con i protocolli precedenti. Ad esempio, utilizza `ELBSecurityPolicy-FS-1-2-Res-2020-10` o la policy più recente disponibile per i listener HTTPS di Application Load Balancer, anziché la policy `ELBSecurityPolicy-2016-08` predefinita. Le policy più recenti richiedono almeno TLS 1.2, segretezza di inoltro e cifrari avanzati compatibili con i browser Web moderni.

Per ulteriori informazioni sulle policy di sicurezza disponibili per gli endpoint pubblici HTTPS, vedi:

- Policy di sicurezza SSL predefinite per Classic Load Balancer (documentazione di Elastic Load Balancing)
- Policy di sicurezza per Application Load Balancer (documentazione di Elastic Load Balancing)
- Protocolli e cifrari supportati tra i visualizzatori e CloudFront (documentazione di CloudFront)

WKLD.14 - Utilizza i servizi di protezione edge per gli endpoint pubblici

Invece di gestire il traffico direttamente da servizi di calcolo come istanze o container EC2, utilizza un servizio di protezione edge. Ciò fornisce un ulteriore livello di sicurezza tra il traffico in entrata da Internet e le risorse che gestiscono tale traffico. Questi servizi possono filtrare il traffico indesiderato, implementare la crittografia e applicare regole di routing o altre regole, come il bilanciamento del carico, prima che il traffico raggiunga le risorse interne.

I servizi AWS in grado di fornire protezione degli endpoint pubblici includono AWS WAF, CloudFront, Elastic Load Balancing, API Gateway ed Amplify Hosting. Esegui servizi basati su VPC, come Elastic Load Balancing, in una sottorete pubblica come un proxy per le risorse dei servizi Web in esecuzione in una sottorete privata.

CloudFront, API Gateway e Amazon Route 53 forniscono protezione dagli attacchi DDoS (Distributed Denial of Service) di livello 3 e 4 gratuitamente e AWS WAF può proteggere dagli attacchi di livello 7.

Le istruzioni per iniziare a utilizzare ciascuno di questi servizi sono disponibili qui:

- Nozioni di base su AWS WAF (sito Web di AWS)
- Nozioni di base su Amazon CloudFront (documentazione di CloudFront)
- Nozioni di base su Elastic Load Balancing (documentazione di Elastic Load Balancing)
- Nozioni di base su API Gateway (documentazione di API Gateway)
- Nozioni di base su Amplify Hosting (documentazione di Amplify)

WKLD.15 - Definisci i controlli di sicurezza nei modelli e distribuiscili utilizzando pratiche CI/CD

Infrastruttura come codice (IaC) è la pratica con cui vengono definite tutte le risorse di servizio e le configurazioni di AWS in modelli e codice distribuiti utilizzando pipeline di integrazione continua e distribuzione continua (CI/CD), le stesse pipeline utilizzate per distribuire applicazioni software. I servizi IaC, come AWS CloudFormation, supportano policy IAM basate sulle identità e sulle risorse e supportano servizi di sicurezza AWS, come Amazon GuardDuty, AWS WAF e Amazon VPC. Acquisisci questi artefatti come modelli IaC, esegui il commit dei modelli in un repository di codice sorgente e quindi distribuiscili utilizzando pipeline CI/CD.

Se non diversamente richiesto, esegui il commit delle policy di autorizzazione delle applicazioni con il codice dell'applicazione nello stesso repository e gestisci le policy generali delle risorse e le configurazioni dei servizi di sicurezza in repository di codice e pipeline di implementazione separati.

Per ulteriori informazioni sulle nozioni di base relative a IaC su AWS, consulta la documentazione di AWS Cloud Development Kit (AWS CDK).

Collaboratori

Hanno collaborato alla stesura del presente documento:

- Jay Michael, Principal Solutions Architect
- Cole Calistra, Principal Solutions Architect
- Justin Plock, Principal Solutions Architect
- Faisal Farooq, Solutions Architect
- Michael Nguyen, Sr. Solutions Architect
- Ritik Khatwani, Sr. Solutions Architect
- Paul Hawkins, Principal, Office of the Chief Information Security Officer (CISO)

Un ringraziamento speciale alle persone che hanno contribuito anche tramite consulenze e revisioni:

- Robert Put
- Mike Sullivan
- Bob Lee III

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
Impostazioni del bucket Amazon S3	Abbiamo aggiornato la sezione ACCT.08 - Impedisci l'accesso pubblico ai bucket S3 privati per indicare che per i bucket Amazon S3 creati dopo il 28 aprile 2023 l'impostazione Blocca accesso pubblico è abilitata per impostazione predefinita.	18 maggio 2023
Best practice sulla sicurezza IAM	Abbiamo aggiornato questa guida per allinearla alle best practice AWS Identity and Access Management (IAM) più recenti. Per ulteriori informazioni, consulta Best practice di sicurezza nella documentazione di IAM.	1 febbraio 2023
Ruoli IAM	Abbiamo fornito collegamenti aggiuntivi alla documentazione di Servizio AWS nella sezione WKLD.01 - Usa i ruoli IAM per le autorizzazioni dell'ambiente di calcolo.	22 settembre 2022
Policy sulle password	Abbiamo aggiornato i suggerimenti per le password sicure in modo da utilizzare le linee guida più recenti del	10 maggio 2022

	Center for Internet Security (CIS).	
Pubblicazione iniziale	—	13 aprile 2022

Glossario del Prontuario AWS

I seguenti termini sono comunemente utilizzati in strategie, guide e pattern forniti dal Prontuario AWS. Per suggerire voci, utilizza il link Fornisci feedback alla fine del glossario.

Numeri

7 R

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

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: esegui la migrazione del database Oracle on-premise ad Amazon Aurora edizione compatibile con PostgreSQL.
- Ridefinire la piattaforma (lift and reshape): trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: esegui la migrazione del database Oracle on-premise ad Amazon Relational Database Service (Amazon RDS) per Oracle nel cloud AWS.
- Riacquistare (drop and shop): passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: esegui la migrazione del tuo sistema di gestione delle relazioni con i clienti (CRM) su Salesforce.com.
- Eseguire il rehosting (lift and shift): trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: esegui la migrazione del tuo database Oracle on-premise su Oracle su un'istanza EC2 nel cloud AWS.
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Questo scenario di migrazione è specifico di VMware Cloud su AWS, che supporta la compatibilità delle macchine virtuali (VM) e la portabilità del carico di lavoro tra l'ambiente on-premise e AWS. È possibile utilizzare le tecnologie VMware Cloud Foundation dai data center on-premise durante la migrazione dell'infrastruttura a VMware Cloud su AWS. Esempio: trasferisci l'hypervisor che ospita il database Oracle su VMware Cloud su AWS.
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a

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

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

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione aggregata

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

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

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

AWS Workload Qualification Framework (AWS WQF)

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

B

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

ramo

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

accesso break-glass

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

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

C

CAF

Vedi AWSCloud Adoption Framework.

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

centro di eccellenza del cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

- Progetto: esecuzione di alcuni progetti relativi al cloud per scopi di dimostrazione e apprendimento
- Fondamento: effettuare investimenti fondamentali per dimensionare l'adozione del cloud (ad esempio, creazione di una zona di destinazione, definizione di un CCoE, definizione di un modello operativo)

- Migrazione: migrazione di singole applicazioni
- Reinvenzione: ottimizzazione di prodotti e servizi e innovazione nel cloud

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

cache fredda

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

dati freddi

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

visione artificiale

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

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

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro,Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Per informazioni su come

utilizzare la progettazione basata sul dominio con il modello del fico strangolatore (Strangler Fig), consulta la sezione Modernizzazione incrementale dei servizi Web Microsoft ASP.NET (ASMX) legacy utilizzando container e il Gateway Amazon API.

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

edge computing

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

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

crittografia envelope

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

ambiente

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

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

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione. Ad esempio le epiche di sicurezza AWS CAF includono la gestione delle identità e degli accessi,

i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS, consulta la guida all'implementazione del programma.

analisi esplorativa dei dati (EDA)

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

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

Quanto è importante una caratteristica per le previsioni di un modello. Di solito viene espresso come punteggio numerico che può essere calcolato con varie tecniche, come Shapley Additive

Explanations (SHAP) e gradienti integrati. Per ulteriori informazioni, vedere Interpretabilità del modello di machine learning con: AWS.

trasformazione delle funzionalità

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

G

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

alta disponibilità (HA)

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

modernizzazione storica

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

I

IaC

Considera l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

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

migrazione incrementale

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

infrastruttura

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

infrastruttura come codice (IaC)

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

Internet delle cose industriale (IIoT)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

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

ramo principale

Vedi filiale.

servizi gestiti

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

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

migrazione su larga scala

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

fabbrica di migrazione

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

MAPPA

Vedi Migration Portfolio Assessment.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

integrazione delle operazioni (OI)

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

trail organizzativo

Un trail creato da AWS CloudTrail che registra tutti gli eventi per tutti gli Account AWS in un'organizzazione di AWS Organizations. Questo percorso viene creato in ogni Account AWS che

fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, vedere Creazione di un percorso per un'organizzazione nella documentazione. CloudTrail

gestione del cambiamento organizzativo (OCM)

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

O

Vedi la revisione della prontezza operativa.

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

Privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

Un controllo di sicurezza progettato per impedire l'implementazione di risorse non conformi. Questi controlli analizzano le risorse prima del loro provisioning. Se la risorsa non è conforme al

controllo, non viene fornita. Per ulteriori informazioni, consulta la guida di riferimento sui controlli nella AWS Control Tower documentazione e consulta Controlli proattivi in Implementazione dei controlli di sicurezza su. AWS

Ambiente di produzione

Vedi ambiente.

pseudonimizzazione

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Regione

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

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

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

S

SAML 2.0

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

SCP

Vedi la politica di controllo del servizio.

Secret

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

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

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

crittografia simmetrica

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

test sintetici

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

T

tags

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

variabile di destinazione

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

elenco di attività

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

Ambiente di test

Vedi ambiente.

training

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

Transit Gateway

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

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

regolazione

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

team da due pizze

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

U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

Gruppi funzionali in un progetto di migrazione responsabili di una serie specifica di attività. Ogni flusso di lavoro è indipendente ma supporta gli altri flussi di lavoro del progetto. Ad esempio, il flusso di lavoro del portfolio è responsabile della definizione delle priorità delle applicazioni,

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

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

vulnerabilità zero-day

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

applicazione zombie

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

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