



Adozione dello standard Matter per i produttori di dispositivi IoT

AWS Guida prescrittiva



AWS Guida prescrittiva: Adozione dello standard Matter per i produttori di dispositivi IoT

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Introduzione	1
Obiettivi	1
Comprendere la materia	3
Protocollo Matter	3
Panoramica di come funziona Matter	4
Vantaggi della certificazione	5
Vantaggi della certificazione Matter per i consumatori di case intelligenti	5
Configurazione semplificata e gestione unificata	6
Migliore scelta e flessibilità nel controllo vocale	6
Vantaggi della certificazione Matter per i produttori di dispositivi	7
Certificazione unica per tutti gli ecosistemi	7
Costi di sviluppo ridotti	7
Assistenza clienti semplificata	8
Considerazioni sulla certificazione	9
Protocolli di connettività non IP	9
Limitazioni hardware	10
Ecosistemi di clienti	11
Tipi di dispositivi non ancora definiti	11
Un'alternativa: invio di proxy ai gateway	12
Connettività cloud con Matter	13
Abilitare funzionalità avanzate dei dispositivi con connettività cloud per gli endpoint Matter	13
Casi d'uso che richiedono la connettività cloud	13
Architetture per abilitare la connettività cloud	15
Hub Smart-home con gateway integrato	15
Trasferisci la connettività cloud a un hub Matter esistente	15
Connettività cloud diretta negli endpoint	15
Bridging Matter e le piattaforme cloud del produttore	16
Sicurezza	17
Autenticazione dei dispositivi	17
Comunicazione crittografata	18
Over-the-air aggiornamenti	18
Sviluppo con Matter	19
Usare Alexa	19
Programma: funziona con Alexa	19

SDK: sviluppa Matter con Alexa	19
Kit: kit per sviluppatori Alexa Ambient Home	19
Endpoint: Endpoint commissionabile	19
CA privata AWS supporto per Matter	19
DAC per Matter	20
Certificati operativi del nodo (NOC)	20
CRL Revoca Support (Matter versione 1.2 e successive)	20
Infrastruttura per Matter	21
Esempi di Java	21
Guida per la conformità a Matter PKI	21
Integrazioni gestite con AWS IoT Device Management	21
FAQs	23
Quali sono i livelli di iscrizione a Matter?	23
In che modo i consumatori di case intelligenti traggono vantaggio da Matter?	23
In che modo i produttori di dispositivi traggono vantaggio da Matter?	23
Matter sostituisce Wi-Fi, Bluetooth o Thread?	24
Cosa sono l'ID del fornitore e l'ID del prodotto?	25
Quali dispositivi devono essere certificati Matter?	25
Il mio tipo di prodotto non è attualmente definito in Matter. Per quali attività aggiuntive devo dedicare del tempo per ottenere la certificazione Matter dei prodotti?	25
Alcuni dei miei dispositivi si connettono direttamente alla rete Wi-Fi domestica. Questi dispositivi devono essere certificati Matter?	26
Qual è la versione attuale di Matter e quali sono le novità?	26
Resources	28
AWS risorse	28
Connectivity Standards Alliance (CSA) per l'IoT	28
Cronologia dei documenti	29
Glossario	30
#	30
A	31
B	34
C	36
D	39
E	43
F	46
G	48

H	49
I	50
L	53
M	54
O	59
P	61
Q	64
R	65
S	68
T	72
U	74
V	74
W	75
Z	76
.....	lxxvii

Adozione dello standard Matter per i produttori di dispositivi IoT

Tushar Patel, Vijay Ujjain e David Walters, Amazon Web Services

Marzo 2026 ([storia](#) del documento)

Secondo [Statista](#), il numero di utenti di smart home in tutto il mondo dovrebbe superare 1,9 miliardi entro il 2029. Questa rapida crescita comporta sfide in termini di operazioni e gestione. Dal punto di vista del consumatore, ogni fornitore di dispositivi utilizza un metodo diverso per integrare il dispositivo per la casa intelligente su una rete domestica tramite un'app specifica per quel fornitore di dispositivi. Ciò rende difficile gestire una gamma crescente di diversi tipi di dispositivi di vari fornitori. Allo stesso modo, dal punto di vista di un produttore di dispositivi, la certificazione dei propri prodotti per la casa intelligente con vari ecosistemi aumenta i costi e la complessità dei processi aziendali. Ad esempio, ciò potrebbe richiedere caratteristiche diverse SKUs per lo stesso modello di dispositivo. Mantenere un'app accattivante per l'esperienza utente e fornire aggiornamenti periodici rappresenta un costo aggiuntivo, sottraendo risorse alla creazione e alla fornitura di un prodotto migliore. Sia i consumatori che i produttori di dispositivi trarrebbero vantaggio da uno standard comune di interoperabilità per le case intelligenti. Questo standard consente ai dispositivi di più fornitori di interagire tra loro in modo semplice, sicuro e affidabile. Sia i consumatori che i produttori di dispositivi hanno tratto vantaggi significativi dall'adozione di uno standard comune di interoperabilità per le case intelligenti che consente ai dispositivi di più fornitori di interagire in modo semplice, sicuro e affidabile.

Lo standard [Matter](#) si è evoluto da un'entusiasmante opportunità per i produttori di dispositivi Internet of Things (IoT) nel settore delle case intelligenti di mantenere effettivamente la promessa di un unico protocollo per connettere i sistemi di casa intelligente. Questo standard mira a migliorare la compatibilità e l'interoperabilità tra dispositivi di produttori diversi. Matter è un protocollo di connettività aperto per la casa intelligente che consente la comunicazione tra dispositivi IoT, app mobili e servizi cloud.

Obiettivi

Quando integrano lo standard Matter nei loro prodotti, i produttori di dispositivi IoT devono affrontare diverse sfide prima di iniziare lo sviluppo. Matter offre molti vantaggi rispetto ai protocolli IoT proprietari, tra cui interoperabilità, sicurezza, semplicità, affidabilità e dispositivi a prova di futuro.

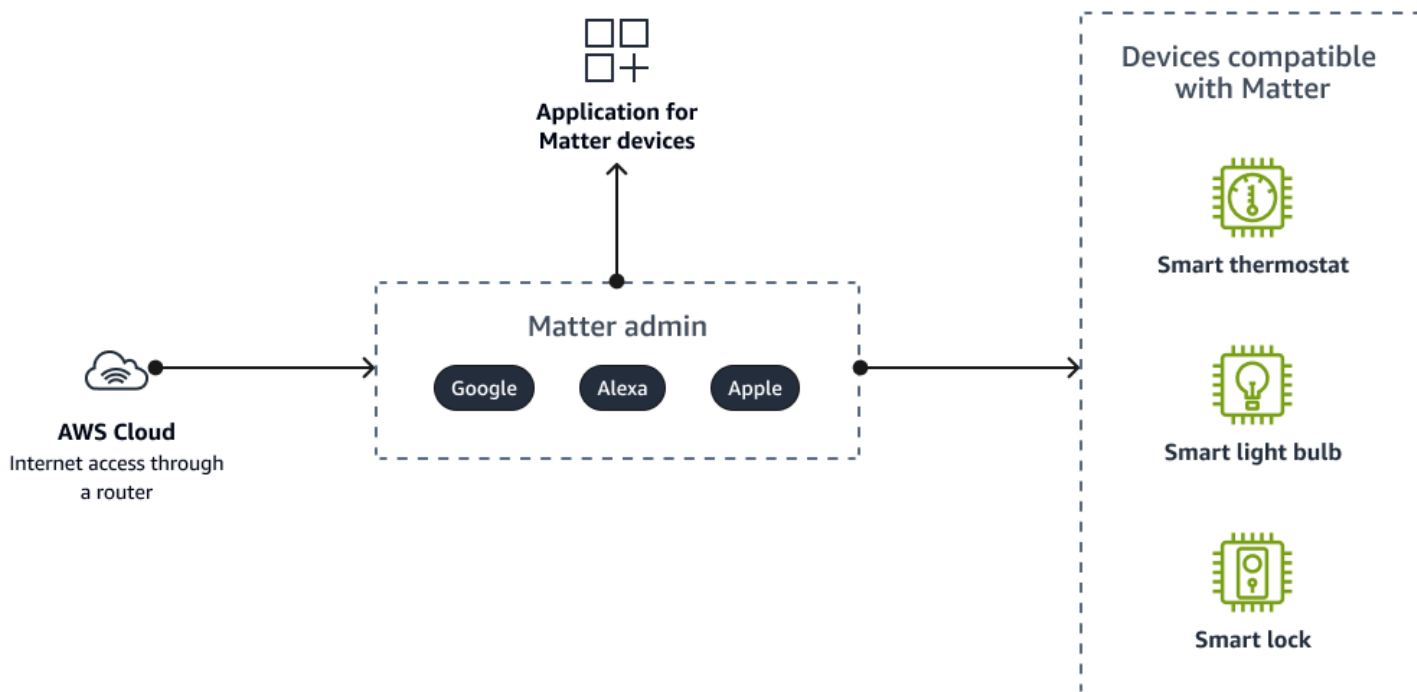
Tuttavia, l'integrazione di Matter nelle implementazioni IoT nuove ed esistenti richiede un'attenta pianificazione e strategia. I produttori desiderano una guida sul processo di conformità di Matter per sfruttare i vantaggi evitando le insidie. Questa guida fornisce ai produttori di dispositivi IoT una guida completa sull'adozione di Matter. Include una tabella di marcia chiara, dalla strategia all'implementazione. Questa guida facilita la transizione a Matter, aiutandoti a creare prodotti sicuri, interoperabili e pronti per il futuro che prosperano nell'ecosistema della casa intelligente. Con il giusto approccio strategico, le organizzazioni possono superare gli ostacoli dell'adozione di Matter e sviluppare dispositivi IoT innovativi che adottano standard aperti.

Lo standard Matter, ora nella versione 1.5, è diventato una soluzione collaudata per i produttori di dispositivi Internet of Things (IoT) nel settore delle case intelligenti. Questo standard aperto ha dimostrato miglioramenti sostanziali nella compatibilità e nell'interoperabilità tra dispositivi di diversi produttori. Matter è un protocollo di connettività aperto per la casa intelligente che consente la comunicazione tra dispositivi IoT, app mobili e servizi cloud nei principali ecosistemi tra cui Amazon Alexa, Google Home, Apple HomeKit e Samsung SmartThings.

Matter 1.5 introduce un supporto esteso per i dispositivi oltre alla versione iniziale, che ora include dispositivi avanzati per la gestione dell'energia, aspirapolvere robotici, sensori di qualità dell'aria, purificatori d'aria e un supporto migliorato per telecamere e sistemi di sicurezza. Lo standard ha anche aggiunto funzionalità avanzate come funzionalità multi-amministrazione, flussi di messa in servizio migliorati e protocolli di sicurezza avanzati. Con migliaia di dispositivi Matter certificati ora disponibili sul mercato, l'ecosistema ha raggiunto una massa critica, rendendo l'adozione di Matter essenziale anziché facoltativa per i produttori di dispositivi che cercano competitività sul mercato.

Questa guida fornisce ai produttori di dispositivi una panoramica completa di Matter e dei passaggi necessari per diventare conformi a Matter. Descrive i pro e i contro della pianificazione di una strategia di adozione di Matter. La guida suggerisce anche le migliori pratiche per sfruttare Matter continuando a supportare i protocolli wireless esistenti, in modo graduale. Per i produttori di dispositivi IoT che esplorano soluzioni per la casa intelligente, questa guida può essere utile per la strategia di connettività.

Comprendere lo standard Matter



Protocollo Matter

Matter è un protocollo di connettività aperto per la casa intelligente che consente la comunicazione tra dispositivi, app mobili e servizi cloud. Sviluppato dalla Connectivity Standards Alliance (CSA), Matter semplifica la connettività e l'interoperabilità per consumatori e produttori. Matter supporta un'ampia gamma di categorie di case intelligenti. Per i consumatori, Matter offre onboarding, gestione unificata e controllo tra gli ecosistemi. Per i produttori, Matter riduce i costi di sviluppo e supporto attraverso un'unica certificazione e lo sviluppo di app. Molte grandi aziende, come Amazon, Apple e Google, stanno promuovendo l'adozione di Matter. CSA offre quattro [livelli di iscrizione](#) a seconda del coinvolgimento dell'organizzazione: promotori, partecipanti, adottanti e associati. Con un forte supporto del settore, Matter mira a fornire una connettività senza interruzioni tra i marchi per i consumatori e a semplificare lo sviluppo per i produttori.

Lo standard Matter per la casa intelligente è maturato in modo significativo con l'introduzione della versione 1.5 il 20 novembre 2025. Lo standard ha esteso il supporto per lo streaming di telecamere e i sistemi di gestione dell'energia tra cui energia solare, batterie e pompe di calore. I progressi a livello di protocollo includono miglioramenti della stabilità per Thread e una migliore integrazione dei dispositivi TV.

Panoramica di come funziona Matter

Matter è un protocollo a livello di applicazione basato su IP per dispositivi domestici intelligenti in tutti gli ecosistemi dei fornitori. Funziona su IPv6 dispositivi che utilizzano. Concettualmente, Matter è organizzato come una raccolta di nodi di rete, che sono gli endpoint di Matter. Di seguito è riportato un breve riassunto della terminologia di Matter:

- I dispositivi Matter sono prodotti per la casa intelligente, come lampadine, interruttori, termostati o serrature.
- Una struttura Matter è la rete virtuale a cui sono collegati tutti i dispositivi. Tutti i dispositivi condividono la stessa root affidabile. Il tessuto forma una topologia di rete a stella.
- Un amministratore di Matter crea, mantiene e gestisce la sicurezza e i privilegi per tutti i dispositivi dell'infrastruttura. Un amministratore può essere un hub o un'applicazione. Matter ha una funzione Multi-Admin, in cui un dispositivo Matter può far parte di più strutture contemporaneamente. Ad esempio, un singolo dispositivo Matter può essere gestito sia da un dispositivo Amazon Alexa che da un dispositivo Google Home, entrambi amministratori Matter sulla stessa rete fisica.
- Un commissario Matter è un dispositivo che mette in servizio (o integra) un nuovo dispositivo Matter nel tessuto. Potrebbe trattarsi di un'app su un telefono, un gateway per la casa intelligente o un amministratore di Matter.
- Un bridge Matter collega i dispositivi con protocollo non IP a una struttura Matter.

Per informazioni sui diversi ruoli che hardware e software possono assumere in Matter, consulta [Peeking Under the Hood of Your Matter Smart Home](#) (post sul blog CSA). La versione 1.4 di Matter ha introdotto Enhanced multi-admin con una migliore condivisione delle credenziali utilizzando Home Router Access Protocol (HRAP). La versione 1.5 di Matter ha introdotto lo streaming tramite videocamera. Le versioni di Matter vengono rilasciate circa due volte all'anno.

Vantaggi della certificazione con Matter

Matter ha offerto vantaggi significativi sia ai consumatori di case intelligenti che ai produttori che li servono. Stabilendo un linguaggio comune per i dispositivi intelligenti, Matter ha affrontato con successo un mercato precedentemente frammentato attraverso una configurazione semplificata, una gestione unificata tra le piattaforme e un'ampia scelta e flessibilità nel controllo vocale.

Per i consumatori, questa esperienza unificata ha reso la costruzione e l'espansione della propria casa intelligente molto meno complesse e scoraggianti. Con migliaia di dispositivi Matter certificati ora disponibili nei principali ecosistemi tra cui Amazon Alexa, Google Home, Apple e Samsung HomeKit SmartThings, la promessa di interoperabilità è diventata realtà. I produttori di dispositivi hanno inoltre ottenuto vantaggi significativi grazie alla certificazione semplificata, alla riduzione dei costi di sviluppo e all'assistenza clienti semplificata.

Dal suo lancio nel 2022, Matter si è evoluto attraverso più versioni. La versione 1.5 di Matter ora supporta oltre 50 tipi di dispositivi, inclusa l'attesissima funzionalità di streaming della videocamera. Lo standard ha raggiunto una massa critica sul mercato, rendendo la certificazione Matter essenziale anziché opzionale per i produttori di dispositivi che cercano competitività. Sia i consumatori che i produttori traggono vantaggio dal fatto che Matter continua a promuovere una maggiore interoperabilità e a ridurre le barriere all'adozione delle case intelligenti. Nel complesso, la certificazione secondo lo standard Matter ha accelerato la crescita del mercato delle case intelligenti risolvendo problemi che in precedenza lo ostacolavano.

Argomenti

- [Vantaggi della certificazione Matter per i consumatori di case intelligenti](#)
- [Vantaggi della certificazione Matter per i produttori di dispositivi](#)

Vantaggi della certificazione Matter per i consumatori di case intelligenti

Matter offre vantaggi significativi per i consumatori. Matter fornisce un linguaggio comune per i dispositivi per la casa intelligente per funzionare insieme senza problemi sulle principali piattaforme. Certificando i dispositivi con Matter, i consumatori ora sperimentano una configurazione e una gestione più semplici della loro casa intelligente, nonché una maggiore flessibilità e scelta nel modo in cui controllare i propri dispositivi.

Configurazione semplificata e gestione unificata

Una delle maggiori frustrazioni che i consumatori devono affrontare è rappresentata dai complessi processi di configurazione e onboarding necessari per far funzionare diversi dispositivi per la casa intelligente e farli lavorare insieme. Ogni dispositivo potrebbe richiedere una propria app proprietaria e un account separato. Per risolvere questo problema, Matter ha abilitato plug-and-play la funzionalità per i dispositivi certificati. L'onboarding dei dispositivi certificati Matter è semplice: basta connettere il dispositivo alla rete domestica locale e quindi utilizzare l'amministratore di Matter, come l'app Alexa, per leggere il codice QR sul dispositivo. Matter 1.4.1 ha introdotto Enhanced Setup Flow con codici QR multidispositivo e onboarding NFC, rendendo il processo ancora più snello.

Questa esperienza di configurazione unificata tramite un'unica app significa che i consumatori non devono più destreggiarsi tra più app separate per gestire diverse marche di dispositivi. Possono visualizzare e controllare tutte le luci, le serrature, i sensori, i termostati, le fotocamere, gli elettrodomestici, i dispositivi di gestione dell'energia e altro ancora certificati da un'unica interfaccia. SmartThings Gli utenti Apple HomeKit, Amazon Alexa, Google Assistant e Samsung traggono tutti vantaggio dalla possibilità di scoprire e controllare i dispositivi Matter senza dover scaricare app del produttore separate. La gestione semplificata dei dispositivi per la casa intelligente attraverso un sistema unificato riduce la complessità per i consumatori e rende molto meno scoraggianti la creazione e l'espansione della configurazione.

Migliore scelta e flessibilità nel controllo vocale

Il controllo vocale è diventato un modo popolare per i consumatori di interagire con i propri dispositivi domestici intelligenti. Tuttavia, oggi la scelta dell'assistente vocale spesso determina quali marche di dispositivi è possibile controllare con la voce. Matter cambia questa situazione abilitando il controllo vocale in tutti gli ecosistemi.

I consumatori ottengono la flessibilità di scegliere l'ecosistema di assistenti vocali più adatto alle loro esigenze, senza doversi preoccupare della compatibilità dei dispositivi. Un utente a proprio agio con l'Assistente Google può controllare i propri dispositivi certificati Matter con la voce, anche se i dispositivi sono stati originariamente prodotti per Alexa o per i mercati. HomeKit

Questa compatibilità incrociata del controllo vocale crea un ambiente più aperto che offre agli utenti una scelta più ampia. Possono scegliere i dispositivi in base alle caratteristiche e ai prezzi anziché alla compatibilità con un singolo ecosistema. Se un utente desidera cambiare assistente vocale in futuro, la configurazione della casa intelligente esistente può facilmente spostarsi con lui perché tutti i dispositivi parlano il linguaggio comune Matter.

La funzionalità Enhanced Multi-Admin aggiunta nella versione 1.4 di Matter consente di controllare un singolo dispositivo da più assistenti vocali contemporaneamente. Ciò significa che i membri della famiglia possono utilizzare il loro assistente vocale preferito (Alexa, Google Assistant o Siri) per controllare gli stessi dispositivi senza conflitti o configurazioni aggiuntive.

Vantaggi della certificazione Matter per i produttori di dispositivi

Oltre ad aiutare i consumatori, la certificazione Matter offre anche vantaggi significativi ai produttori di dispositivi intelligenti. Adottando lo standard Matter, le organizzazioni possono ottenere vantaggi che riducono i costi e ampliano la portata dei clienti. Dal lancio di Matter nel 2022 e dall'evoluzione fino alla versione 1.5 (novembre 2025), questi vantaggi sono stati realizzati dai produttori di tutto il settore delle case intelligenti

Certificazione unica per tutti gli ecosistemi

Per garantire la compatibilità tra ecosistemi come Alexa HomeKit, Google Home e Samsung SmartThings, i produttori devono seguire diversi processi di certificazione lunghi e costosi con ciascuna organizzazione. Matter cambia questa situazione stabilendo un'unica certificazione comune.

I produttori di dispositivi devono certificare i propri prodotti una sola volta secondo lo standard Matter per essere compatibili con tutti i principali ecosistemi di case intelligenti e assistenti vocali. Ciò semplifica lo sviluppo e riduce significativamente i costi di certificazione rispetto allo status quo. Non è più necessario spendere risorse per mantenere certificazioni separate man mano che i prodotti vengono aggiornati. Una certificazione Single Matter rende inoltre i prodotti a prova di futuro e garantisce la compatibilità anche quando emergono nuovi ecosistemi.

Il CSA ha inoltre migliorato il processo di certificazione con strumenti migliori, tra cui Certification Tool, PICS Tool e ZUTH, oltre a reti ampliate di fornitori di test e a una struttura di test di interoperabilità.

Costi di sviluppo ridotti

Matter aiuta anche a ridurre i costi di sviluppo per i produttori. Adottando uno standard di connettività e sicurezza comune, le organizzazioni beneficiano di componenti di infrastruttura condivisi che contribuiscono all'intero progetto Matter.

Ad esempio, i produttori non devono più includere i propri router Thread border proprietari nei prodotti, scaricando questa responsabilità sui produttori di hub. I driver e le librerie condivisi e

open source riducono ulteriormente il lavoro di progettazione ridondante. I meccanismi comuni di individuazione dei servizi e di configurazione dei dispositivi implicano lo sviluppo di app meno personalizzate. Queste riduzioni dei costi di sviluppo delle infrastrutture e delle app possono essere trasferite ai consumatori sotto forma di dispositivi per la casa intelligente più convenienti.

L'SDK Matter è maturato in modo significativo rispetto alla versione iniziale, con strumenti di sviluppo, librerie e documentazione completi ora disponibili. La versione 1.4.2 di Matter (giugno 2025) ha introdotto importanti miglioramenti per l'affidabilità del trasporto, la messa in servizio BLE e l'infrastruttura di crittografia e test basata su PSA. Questi miglioramenti hanno ridotto la complessità dell'integrazione rispetto alle fasi iniziali di adozione, accelerando l'introduzione di nuovi prodotti. time-to-market

Matter ora supporta oltre 50 tipi di dispositivi nelle versioni da 1.0 a 1.5, tra cui illuminazione, serrature, termostati, elettrodomestici (frigoriferi, lavastoviglie, forni, microonde), aspirapolvere robotici, dispositivi di gestione dell'energia (pannelli solari, batterie, pompe di calore), caricabatterie per veicoli elettrici, dispositivi di gestione dell'acqua, sensori di qualità dell'aria e telecamere con supporto per lo streaming.

Assistenza clienti semplificata

L'attuale frammentazione del mercato delle case intelligenti comporta elevati oneri di assistenza clienti per i produttori. I consumatori incontrano spesso problemi di connettività, configurazione e compatibilità che richiedono la risoluzione dei problemi. Matter mira a ridurre questi problemi standardizzando le funzioni principali.

Quando si verificano problemi, i comuni protocolli Matter alla base consentono alle aziende di diagnosticare e risolvere più facilmente i problemi di connettività senza dover considerare più ecosistemi. Questo semplifica il processo di supporto. Grazie a un'unica app e alla compatibilità vocale comune, i clienti possono inoltre imparare più facilmente a usare i dispositivi, riducendo la necessità di supporto in molti casi. L'esperienza cliente semplificata e la risoluzione dei problemi offerte da Matter aiutano a ridurre i costi di assistenza a lungo termine per i produttori.

Considerazioni sulla strategia di certificazione

Matter consente l'interoperabilità tra diversi dispositivi e piattaforme per la casa intelligente. Tuttavia, la certificazione con Matter potrebbe non essere sempre la scelta migliore per i produttori di dispositivi. I costi di implementazione e certificazione potrebbero non avere senso pratico o finanziario, a seconda del tipo di dispositivo e dei casi d'uso. Questa sezione illustra alcuni dei motivi principali per cui un produttore potrebbe scegliere di non certificare determinati dispositivi con Matter.

Sebbene lo standard Matter miri a semplificare lo sviluppo e consentire la compatibilità universale, alcuni tipi di dispositivi per la casa intelligente possono incontrare ostacoli pratici alla certificazione che superano i vantaggi. Per i prodotti con vincoli rigorosi, protocolli non IP, un pubblico limitato o tipi di dispositivi non definiti in Matter, inizialmente la certificazione Matter potrebbe non essere la strategia migliore. Queste potrebbero essere le ragioni per cui un produttore potrebbe evitare di adottare Matter. Tuttavia, Matter consente ai dispositivi gateway abilitati all'IP di eseguire il proxy per endpoint non IP. Per alcuni dispositivi legacy, un approccio gateway può essere un percorso praticabile per la compatibilità con Matter, evitando al contempo una riprogettazione completa del dispositivo.

A partire dal 2026, con Matter ora alla versione 1.5 e migliaia di dispositivi certificati sul mercato, l'ecosistema è maturato in modo significativo. Le barriere alla certificazione sono state ridotte grazie a una documentazione migliore e migliorata SDKs e all'ampliamento dell'infrastruttura di test. Tuttavia, le considerazioni descritte di seguito rimangono pertinenti per i produttori che valutano la loro strategia di certificazione.

Man mano che lo standard Matter si evolve e il suo ambito di applicazione si estende per coprire più casi d'uso, le ragioni a favore della certificazione potrebbero rafforzarsi nel tempo, anche per queste categorie di prodotti. I produttori di dispositivi devono valutare le situazioni e le tabelle di marcia specifiche per determinare l'approccio migliore per quanto riguarda la conformità a Matter. In molte situazioni, potrebbero esserci valide ragioni tecniche o commerciali per rinunciare alla certificazione, almeno temporaneamente.

Protocolli di connettività non IP

Per adottare lo standard Matter, i dispositivi devono funzionare su reti IP, come Wi-Fi, Ethernet e Thread. I protocolli wireless non IP, come Zigbee, Z-Wave e Bluetooth LE, sono comunemente usati nei dispositivi a bassa larghezza di banda. Questi protocolli richiedono un traduttore di

protocollo aggiuntivo da non IP a IP per essere compatibili con Matter. L'aggiornamento del modulo di comunicazione o l'introduzione di un gateway di traduzione in genere aumentano il costo hardware del dispositivo.

L'aggiunta del supporto per lo stack IP significa allocare più memoria e potenza di elaborazione per la gestione della rete. Ciò potrebbe superare le capacità dei dispositivi estremamente economici e a basso consumo. L'aggiunta di memoria o flash aggiuntiva per supportare l'IP aumenterebbe anche i costi di produzione e ridurrebbe la durata della batteria. Nei casi d'uso in cui sono necessari solo l'accensione e lo spegnimento dell'alimentazione o i dati dei sensori, i protocolli non IP possono fornire una soluzione efficiente.

Matter esclude essenzialmente la certificazione di tutti i dispositivi che si basano su standard wireless proprietari non IP. Ciò potrebbe limitare i produttori che desiderano utilizzare metodi di connettività alternativi per i loro prodotti di fascia bassa. Sebbene i protocolli basati su IP come Wi-Fi ed Ethernet siano necessari per interfacciare diversi ecosistemi, gli standard non IP sono ancora validi per la connettività di base di sensori e switch in alcune applicazioni.

I Matter bridge sono diventati più comuni e standardizzati, il che consente ai produttori di mantenere le linee di dispositivi non IP esistenti, ottenendo al contempo la compatibilità con Matter attraverso prodotti bridge certificati. Questo approccio si è dimostrato efficace per gli ecosistemi di dispositivi Zigbee e Z-Wave, in cui un singolo bridge può esporre più dispositivi legacy come endpoint Matter.

Limitazioni hardware

Un'altra sfida è che Matter richiede un livello minimo di potenza di elaborazione e memoria sul dispositivo per supportare lo stack software necessario. Tuttavia, i dispositivi per la casa intelligente di base hanno spesso funzionalità di chip integrati molto limitate, a causa dei vincoli di costi e dimensioni.

Ad esempio, un semplice sensore per porte o finestre potrebbe contenere solo un microcontrollore con meno di 100 KB di memoria flash e 10 KB di RAM. Ciò non offre spazio di archiviazione ed elaborazione sufficiente per un'implementazione completa di Matter. L'aggiunta di silicio più potente e costoso farebbe aumentare notevolmente la fattura dei materiali.

Nei casi in cui costi e dimensioni sono le priorità principali, i produttori potrebbero scoprire che i requisiti di Matter non sono in linea con i loro budget hardware. La certificazione di sensori, switch o controller di base con Matter potrebbe imporre aggiornamenti hardware non necessari che influiscono sulla convenienza.

Matter 1.4.2 (giugno 2025) ha introdotto miglioramenti all'affidabilità del trasporto e alla messa in servizio di Bluetooth Low Energy (BLE) che hanno ottimizzato l'utilizzo delle risorse. La maturità dell'SDK e la disponibilità di implementazioni di riferimento hanno inoltre ridotto il sovraccarico dell'integrazione con Matter. Tuttavia, per i dispositivi estremamente limitati (meno di 100 KB di memoria flash), l'approccio gateway proxy rimane la soluzione più pratica.

Ecosistemi di clienti

Un altro fattore da considerare è se la base di clienti target di un produttore utilizza piattaforme per la casa intelligente compatibili con Matter. Se la maggior parte dei consumatori di quel segmento non utilizza i controller Matter o gli hub e le app compatibili con Matter, potrebbero esserci pochi incentivi a certificare i prodotti.

Ad esempio, un'azienda che si concentra sulle esigenze degli utenti anziani potrebbe scoprire che i propri clienti dispongono di configurazioni semplici senza amministratori Matter. Oppure gli appassionati di domotica do-it-yourself (fai-da-te) potrebbero preferire soluzioni personalizzate e non aver bisogno dell' plug-and-play esperienza di Matter in tutti i marchi.

Negli scenari in cui il gruppo demografico target non interagisce con l'infrastruttura Matter, la certificazione aggiunge complessità senza vantaggi evidenti. Le risorse potrebbero essere spese meglio per ottimizzare l'esperienza utente all'interno delle piattaforme pertinenti invece di dedicare gli sforzi alla conformità con Matter.

A partire dal 2026, l'adozione di Matter ha raggiunto la massa critica con i principali ecosistemi (Amazon Alexa, Google Home, Apple HomeKit, Samsung SmartThings) che supportano pienamente lo standard. La consapevolezza dei consumatori nei confronti di Matter è cresciuta in modo significativo e il logo Matter è diventato un marchio riconosciuto di interoperabilità. La domanda demografica target si è spostata da «I clienti usano Matter?» a «Possiamo permetterci di non supportare Matter?» poiché diventa un'aspettativa di base in molti segmenti di mercato.

Tipi di dispositivi non ancora definiti

Sebbene l'ambito di applicazione di Matter si sia notevolmente ampliato rispetto alla versione iniziale, coprendo le categorie più comuni di case intelligenti e molti elettrodomestici, alcuni settori verticali di nicchia attendono ancora la standardizzazione.

Se un'azienda sviluppa tipi di dispositivi unici che non sono coperti dai profili Matter esistenti, la certificazione non è possibile fino a quando non vengono redatti nuovi profili. Ciò potrebbe ritardare il lancio di un nuovo prodotto in attesa che Matter ne amplii l'ambito di applicazione.

Anziché ritardare il lancio di innovazioni, alcuni produttori potrebbero preferire introdurre sul mercato soluzioni di nicchia più rapidamente attraverso mezzi proprietari. La certificazione in un secondo momento è ancora possibile dopo la maturità dei profili pertinenti. Per avere vantaggi da principiante, in alcuni casi potrebbe essere preferibile direct-to-consumer rinunciare a Matter.

Un'alternativa: invio di proxy ai gateway

In situazioni in cui un dispositivo endpoint presenta limitazioni che impediscono la certificazione diretta di Matter, un approccio alternativo consiste nel delegare la funzionalità Matter del dispositivo a un gateway. Il gateway funge da ponte che fa da ponte tra il protocollo wireless locale dell'endpoint e il protocollo Matter basato su IP.

Ad esempio, un sensore di temperatura di base che comunica tramite uno standard radio proprietario potrebbe comunque apparire come dispositivo Matter all'amministratore di Matter. Il gateway riceve i dati dei sensori su un'interfaccia non IP ma espone ai controller le entità Matter virtuali che rappresentano tali dati tramite IP. Ciò consente di utilizzare l'hardware esistente e ottenere alcuni vantaggi di interoperabilità tramite il gateway.

Naturalmente, ciò aggiunge complessità per gli sviluppatori e richiede gateway che supportino il livello di traduzione necessario. Ma potrebbe essere un valido compromesso nei casi in cui la certificazione diretta sia troppo impegnativa per il dispositivo stesso. I proxy potrebbero aiutare le soluzioni a basso consumo o di nicchia a partecipare agli ecosistemi Matter senza una revisione completa dell'hardware.

Le specifiche Matter Bridge sono maturate e numerosi prodotti bridge certificati sono ora disponibili presso i principali produttori. Ciò ha reso l'approccio gateway più praticabile e standardizzato rispetto ai primi giorni di Matter. I produttori possono ora collaborare con fornitori di bridge o sviluppare i propri bridge certificati per integrare i dispositivi non IP nell'ecosistema Matter senza riprogettare l'hardware degli endpoint.

Connettività cloud con Matter

Sebbene Matter consenta l'interoperabilità di base dei dispositivi locali, è necessaria una connettività cloud aggiuntiva per fornire over-the-air aggiornamenti affidabili, dati di telemetria, gestione remota e integrazione con i servizi dei fornitori proprietari. I produttori di dispositivi hanno a disposizione diverse opzioni, come la spedizione di un hub gateway Matter, l'utilizzo di un hub domestico certificato Matter o l'integrazione della connettività cloud diretta negli endpoint. Gli standard per la Matter-to-cloud connettività stanno emergendo, ma i produttori devono ancora integrare stack software di connettività aggiuntivi nei dispositivi Matter. Offrire il massimo valore dei dispositivi per la casa intelligente in aree come la diagnostica e gli aggiornamenti di nuove funzionalità richiede ai produttori di Matter di prendere in considerazione l'integrazione nel cloud, oltre alle operazioni locali di base.

Abilitare funzionalità avanzate dei dispositivi con connettività cloud per gli endpoint Matter

Lo standard Matter promette di unificare i dispositivi IoT di diversi fornitori attraverso un protocollo comune. Specifica in che modo i dispositivi per la casa intelligente scoprono, comunicano e interagiscono tra loro sulla rete locale utilizzando tecnologie di rete basate su IP, come Ethernet, Wi-Fi e Thread. Questa interoperabilità locale consente ai dispositivi certificati Matter di diversi fornitori di lavorare insieme senza problemi per attività come scene automatizzate e controllo vocale. Tuttavia, Matter non definisce le interfacce cloud né richiede la connettività Internet per gli endpoint del dispositivo.

Molti dispositivi intelligenti oggi si basano su una connettività cloud aggiuntiva per funzionalità chiave, come gli aggiornamenti over-the-air (OTA), l'accesso remoto e le integrazioni con le piattaforme dei produttori. I produttori di dispositivi che desiderano creare prodotti conformi a Matter pur mantenendo funzionalità avanzate devono affrontare alcune considerazioni di progettazione relative all'integrazione di Matter con la connettività cloud. Sebbene l'integrazione di base del controllo locale e dell'assistente vocale funzioni per semplici dispositivi Matter, è necessaria una connettività cloud aggiuntiva per abilitare funzionalità più avanzate.

Casi d'uso che richiedono la connettività cloud

Sebbene Matter gestisca l'interoperabilità dei dispositivi locali, la connettività cloud aggiuntiva consente diverse importanti funzionalità dei dispositivi per la casa intelligente:

- **Over-the-air Aggiornamenti (OTA):** la distribuzione di aggiornamenti firmware e software tramite Internet consente ai fornitori di migliorare facilmente i dispositivi già distribuiti. Senza OTA, gli aggiornamenti verrebbero gestiti manualmente. Sebbene lo standard Matter descriva come gli aggiornamenti OTA vengono gestiti e consegnati agli endpoint certificati Matter, ciò dipende dalla funzionalità supportata dall'hub Matter a cui è connesso l'endpoint. Inoltre, esistono restrizioni relative agli aggiornamenti forniti all'endpoint. Ad esempio, quando l'endpoint richiede un aggiornamento, viene fornito solo l'ultimo aggiornamento disponibile. A tutti i dispositivi dello stesso tipo viene fornito un unico aggiornamento. Non è possibile eseguire un aggiornamento sequenziale e nemmeno un rollback OTA o l'eliminazione di un aggiornamento. L'abilitazione della connettività cloud sull'endpoint può mitigare questa mancanza di gestione granulare degli aggiornamenti OTA. La versione 1.4.2 di Matter (giugno 2025) ha introdotto miglioramenti all'affidabilità del trasporto e all'infrastruttura di test che hanno migliorato i meccanismi di aggiornamento OTA. Tuttavia, permangono le limitazioni fondamentali relative agli aggiornamenti sequenziali e alle funzionalità di rollback, il che rende la connettività cloud diretta preziosa per i produttori che richiedono funzionalità granulari di controllo degli aggiornamenti e di gestione del parco veicoli.
- **Streaming e contenuti multimediali:** la versione 1.5 di Matter (novembre 2025) ha introdotto il supporto delle telecamere utilizzando protocolli a canale laterale, come Real-Time Streaming Protocol (RTSP) tramite Wi-Fi o Ethernet. Mentre Matter gestisce l'individuazione dei dispositivi e il controllo di base, lo streaming video effettivo avviene tramite protocolli separati. Ciò richiede spesso un'infrastruttura cloud per la visualizzazione e la registrazione remota e funzionalità basate sull'intelligenza artificiale, come il rilevamento delle persone.
- **Accesso e controllo remoti:** l'accesso e il controllo dei dispositivi in remoto dall'esterno della rete domestica richiede un endpoint cloud. Matter, come attualmente definito, supporta solo l'accesso locale. Sebbene un endpoint Matter possa essere controllato con un'app utente all'interno della rete locale, il controllo remoto è disponibile solo se è supportato dall'hub Matter. Anche in questo caso, in genere, sono disponibili solo telecomandi di base.
- **Telemetria e diagnostica:** l'aggregazione di dati sul campo, come registri di errori e flussi di sensori, nel cloud consente ai fornitori di monitorare lo stato dei dispositivi e identificare i problemi. Sebbene Matter supporti la diagnostica radio e relativa al protocollo tramite il cluster di diagnostica generale, qualsiasi diagnostica dettagliata specifica del dispositivo richiede la connettività cloud in modo che il produttore possa recuperare i dati dal dispositivo.
- **Integrazioni specifiche del fornitore:** tutte le funzionalità e i tipi di dati personalizzati non definiti nelle specifiche Matter richiedono la connettività alle piattaforme cloud del fornitore. Ciò è particolarmente importante per i dispositivi con funzionalità avanzate come fotocamere (Matter versione 1.5), dispositivi di gestione dell'energia (Matter versione 1.4) ed elettrodomestici (versioni

Matter 1.2-1.3) che potrebbero richiedere servizi cloud specifici del produttore per la piena funzionalità.

- Integrazioni esterne: il collegamento a servizi di terze parti come assistenti vocali non presenti nell'ecosistema Matter o gateway di pagamento di terze parti (a seconda del caso d'uso) richiede una connettività Internet oltre all'amministratore di Matter.

Poiché queste funzionalità critiche si basano sulla connettività cloud, gli endpoint Matter spesso necessitano di opzioni aggiuntive per l'accesso a Internet.

Architetture per abilitare la connettività cloud

Per i dispositivi Matter, esistono tre approcci generali per fornire la connettività cloud necessaria rispettando al contempo le specifiche operative locali.

Hub Smart-home con gateway integrato

Alcuni produttori di dispositivi potrebbero scegliere di fornire un hub domestico proprietario che incorpori sia l'amministratore Matter che un gateway per i propri servizi cloud. Questo hub domestico gestirebbe localmente gli endpoint Matter collegati secondo lo standard, facilitando al contempo le connessioni cloud per funzioni avanzate. L'hub potrebbe supportare gli aggiornamenti OTA, l'accesso remoto e la raccolta di telemetria per gli endpoint.

Trasferisci la connettività cloud a un hub Matter esistente

Invece di raggruppare un hub personalizzato, i dispositivi potrebbero essere progettati per connettersi agli hub Matter, come Amazon Echo, Google Nest Hub, Apple o Samsung SmartThings Hub HomePod, per la connettività Internet. In questo caso, l'hub Matter esistente gestisce la comunicazione con i dispositivi locali secondo lo standard e fornisce anche un gateway verso il cloud per gli endpoint che lo richiedono. Ciò sfrutta l'infrastruttura che i consumatori potrebbero già disporre. Tuttavia, questo approccio dipende dal livello di supporto offerto dall'hub Matter per le funzionalità che non sono specificate come normative per gli hub Matter nello standard.

Connettività cloud diretta negli endpoint

I dispositivi con connettività Internet diretta, come il Wi-Fi, potrebbero integrare una connettività separata per la rete locale Matter e per i servizi cloud dei fornitori. Ciò consente al dispositivo di fungere da gateway indipendente verso il cloud. Tuttavia, sono necessarie soluzioni per gli non-Wi-

Fi endpoint che si basano su protocolli come Thread. Ciò consente ai dispositivi di connettersi al cloud in modo indipendente, ma potrebbe non essere fattibile per dispositivi semplici, a basso costo e alimentati a batteria.

Bridging Matter e le piattaforme cloud del produttore

Sebbene Matter semplifichi l'interoperabilità locale, sono necessari ulteriori sforzi per connettere senza problemi i sistemi di amministrazione Matter e le piattaforme cloud dei produttori. La Connectivity Standards Alliance (CSA) continua a sviluppare standard per la connettività. Matter-to-cloud A partire dal 2026, mentre gli standard formali di interfaccia cloud sono ancora in evoluzione, le migliori pratiche del settore sono emerse dall'implementazione di migliaia di dispositivi Matter. L'adozione su larga scala di standard per questa connettività cloud faciliterebbe lo sviluppo per i produttori di dispositivi.

Il percorso ottimale dipende dai casi d'uso, dai prezzi e dai modelli di business di prodotti specifici. È chiaro che è necessario un accesso affidabile ai servizi cloud per sbloccare tutte le funzionalità che i consumatori di case intelligenti si aspettano, anche per i dispositivi conformi a Matter e incentrati sull'interoperabilità locale. I produttori di dispositivi hanno l'opportunità di utilizzare Matter per l'interoperabilità, pur fornendo funzionalità avanzate attraverso una connettività cloud progettata con cura.

Considerazioni sulla sicurezza per lo standard Matter

La sicurezza fin dalla progettazione è la pratica di incorporare le funzioni di sicurezza durante la fase di progettazione del dispositivo, piuttosto che come elemento secondario durante le fasi successive dello sviluppo. Le comunicazioni crittografate e gli aggiornamenti over-the-air (OTA) sono esempi di sicurezza fin dalla progettazione. Matter fornisce una solida base per i dispositivi domestici intelligenti implementando la sicurezza fin dalla progettazione, a partire da un impianto di produzione affidabile e sicuro. I dispositivi Matter possono essere prodotti e forniti solo dai proprietari di un'autorità di certificazione (CA) nota e affidabile della Product Attestation Authority (PAA).

A partire dalla versione 1.5 di Matter, il framework di sicurezza è stato continuamente rafforzato attraverso più versioni. Matter 1.4.2 (giugno 2025) ha introdotto miglioramenti crittografici basati su PSA, migliorando le basi di sicurezza. La Connectivity Standards Alliance (CSA), che supervisiona lo standard Matter, mantiene un programma di segnalazione delle vulnerabilità dedicato per gestire le divulgazioni di sicurezza per i suoi protocolli.

Autenticazione dei dispositivi

I dispositivi Matter devono autenticarsi tra loro e con un controller prima di poter comunicare. Solo i dispositivi autorizzati possono connettersi alla struttura Matter. Durante la produzione, ai dispositivi viene fornita un'identità univoca e un certificato X.509 noto come Device Attestation Certificate (DAC). Quando il dispositivo tenta di connettersi alla struttura Matter per la prima volta, il dispositivo commissario verifica la validità del DAC e verifica che sia firmato da una CA PAI (Product Attestation Intermediate) nota e affidabile. Il dispositivo del commissario verifica inoltre se il dispositivo che tenta di connettersi alla rete è conforme alle specifiche, ai protocolli e agli standard di sicurezza di Matter. Al dispositivo viene concesso l'accesso alla struttura Matter solo se tutti i controlli hanno esito positivo.

Il CSA mantiene un elenco di autorità di attestazione dei prodotti autorizzate (PAAs) e le pubblica tramite il Distributed Compliance Ledger (DCL). Il DCL è un sistema basato su blockchain che fornisce registrazioni trasparenti e a prova di manomissione dei dispositivi certificati e delle autorità di certificazione affidabili. I produttori possono richiedere di diventare PAAs o collaborare con gli esistenti autorizzati a fornire i propri dispositivi. PAAs Il DCL supporta anche gli Observer Nodes che le parti interessate possono utilizzare per monitorare l'ecosistema di certificazione.

Comunicazione crittografata

Dopo aver concesso al dispositivo l'accesso alla struttura Matter, tutti i dati trasmessi tra i dispositivi sono protetti da una crittografia avanzata. L'integrità dei dati viene preservata utilizzando un approccio a più livelli. Il Matter Commissioner esegue lo scambio di chiavi e la verifica della firma utilizzando la curva ECC-256 secp256r1. Dopo lo scambio delle chiavi, i dispositivi Matter crittografano i dati in transito utilizzando AES-256. Per ogni messaggio, i dispositivi utilizzano l'algoritmo SHA-256 per verificare che i dati non siano stati manomessi durante la trasmissione.

La versione 1.4 di Matter ha introdotto funzionalità Multi-Admin avanzate con Home Router Access Protocol (HRAP). Ciò ha migliorato la sicurezza per gli scenari in cui i dispositivi sono controllati da più ecosistemi contemporaneamente. Questo miglioramento garantisce che la condivisione delle credenziali e il controllo degli accessi rimangano sicuri anche quando un dispositivo partecipa a più strutture Matter. Ogni struttura mantiene il proprio contesto di sicurezza, impedendo che la compromissione in un ecosistema influisca sugli altri.

Over-the-air aggiornamenti

Lo standard Matter richiede inoltre che i dispositivi implementino una solida posizione di sicurezza per gli aggiornamenti over-the-air (OTA). L'OTA è una parte fondamentale di un ecosistema di case intelligenti in modo che i dispositivi possano ricevere aggiornamenti di sicurezza insieme a nuove funzionalità. Ogni aggiornamento del firmware per i dispositivi Matter deve essere firmato con la chiave privata del produttore. Il dispositivo verifica la firma del payload utilizzando la chiave pubblica asimmetrica corrispondente. Dopo aver verificato la firma del payload, il dispositivo può salvare l'immagine nel bootloader e resettarla. Durante il processo di avvio, il dispositivo deve verificare nuovamente l'immagine per assicurarsi che non sia stata manomessa e deve inoltre verificare che stia eseguendo l'ultima versione nota.

La versione 1.4.2 di Matter (giugno 2025) ha introdotto miglioramenti significativi all'infrastruttura di aggiornamento OTA, tra cui una migliore affidabilità del trasporto e framework di test avanzati. Questi miglioramenti hanno reso gli aggiornamenti OTA più robusti e affidabili nelle implementazioni di produzione. Tuttavia, i produttori dovrebbero tenere presente che il meccanismo OTA di Matter presenta limitazioni per quanto riguarda gli aggiornamenti sequenziali e le funzionalità di rollback. Per i dispositivi che richiedono un controllo granulare degli aggiornamenti, la gestione del parco veicoli o il A/B test del firmware, i produttori potrebbero dover integrare l'OTA di Matter con una connettività cloud diretta alla propria infrastruttura di aggiornamento.

Sviluppo con Matter

Usare Alexa

Amazon offre una suite completa di strumenti per lo sviluppo di Matter. Questi strumenti forniscono un percorso rapido per creare prodotti Matter compatibili con tutti i principali ecosistemi e che funzionano perfettamente con Amazon Alexa.

Programma: funziona con Alexa

Questo programma assicura che i dispositivi connessi ad Alexa offrano un'esperienza cliente eccezionale. Il badge Works with Alexa (WWA) aumenta la fiducia dei clienti, il che aiuta a favorire la preferenza per i dispositivi certificati. Per ulteriori informazioni, consulta [Annuncio del lancio di Matter e Introduzione a Works with Alexa \(WWA\) per i dispositivi Matter](#) (post sul blog di Amazon).

SDK: sviluppa Matter con Alexa

Questo SDK ti consente di aggiungere la connettività Matter locale al tuo dispositivo, includendo anche connettività cloud gestita, business intelligence e supporto OTA. Per ulteriori informazioni, consulta [Ottieni il massimo da Matter con Alexa](#).

Kit: kit per sviluppatori Alexa Ambient Home

Questo kit ti aiuta a integrarti con dispositivi diversi protocolli per creare una casa intelligente ambientale e unificata con Alexa. Per ulteriori informazioni, consulta [Amazon Alexa](#).

Endpoint: Endpoint commissionabile

Per i dispositivi Matter connessi tramite skill, l'API Commissionable Endpoint crea una connessione locale basata su Matter ai dispositivi Alexa senza che il cliente richieda alcuna procedura con la sua autorizzazione. Per ulteriori informazioni, consulta [Alexa.Commissionable Interface 1.0 \(Alexa Skills Kit\)](#).

CA privata AWS supporto per Matter

AWS Autorità di certificazione privata (CA privata AWS) fornisce indicazioni sull'uso dello standard Matter.

DAC per Matter

Matter richiede un certificato di attestazione del dispositivo (DAC), che deve essere rilasciato da una CA di attestazione del dispositivo conforme alla politica di certificazione (CP) dell'infrastruttura a chiave pubblica (PKI) di Matter. I fornitori di dispositivi possono utilizzare per effettuare le seguenti operazioni: CA privata AWS

- Ospita l'autorità di certificazione (CA) della Product Attestation Authority (PAA)
- Ospita la CA Product Attestation Intermediate (PAI)
- Emetti, firma e gestisci il DAC di ogni dispositivo

Per ulteriori informazioni, consulta [Utilizzare per AWS Autorità di certificazione privata emettere certificati di attestazione dei dispositivi per Matter](#) nel AWS Security Blog.

Certificati operativi del nodo (NOC)

Oltre all'attestazione del dispositivo, AWS Private CA supporta l'emissione di certificati operativi Node (NOCs), che vengono utilizzati per proteggere le comunicazioni all'interno di una struttura Matter. AWS fornisce esempi Java per l'attivazione di una CA radice e una CA subordinata e la creazione di un NOCs NOC.

Per ulteriori informazioni, consulta [Usare l' CA privata AWS API per implementare i certificati Matter nella documentazione](#). AWS Autorità di certificazione privata

CRL Revoca Support (Matter versione 1.2 e successive)

La versione 1.2 di Matter ha introdotto la revoca del Device Attestation Certificate (DAC) utilizzando Certificate Revocation Lists (). CRLs Quando si abilita la revoca CRL per CAs quell'emissione, i certificati Matter, impostateli `true` nell'oggetto `OmitExtension` all'interno della struttura. `CrlConfiguration CrlDistributionPointExtensionConfiguration` In Matter, l'URI CRL Distribution Point (CDP) non è incorporato nei certificati ma viene invece recuperato dal Matter Distributed Compliance Ledger (DCL). È necessario caricare l'URI CDP su Matter DCL per scoprirlo durante la convalida del DAC.

Infrastruttura per Matter

AWS fornisce un esempio che dimostra l'utilizzo di [AWS Cloud Development Kit \(AWS CDK\)](#) per configurare l'infrastruttura PKI per Matter. Si utilizza CA privata AWS per soddisfare i requisiti del Matter PKI CP. Per ulteriori informazioni, consulta il progetto [Matter PKI CDK](#) su GitHub

Esempi di Java

CA privata AWS fornisce esempi Java per la creazione di certificati PAA (Product Attestation Authority) conformi a Matter, certificati PAI (Product Attestation Intermediate) e Device Attestation Certificates (). DACs Per ulteriori informazioni, consulta [Utilizzo dell' CA privata AWS API per implementare](#) lo standard Matter (esempi Java) nella documentazione. AWS Autorità di certificazione privata

Guida per la conformità a Matter PKI

Questa [guida alla conformità di Matter PKI](#) spiega come implementare e dimostrare la conformità ai requisiti CSA Matter PKI CP. Fornisce informazioni su come è possibile utilizzare per creare e gestire autorità di certificazione conformi CA privata AWS a Matter (). CAs

Integrazioni gestite con AWS IoT Device Management

[AWS IoT Device Management](#) include la funzionalità di integrazioni gestite, che fornisce un'interfaccia unificata per l'onboarding e la gestione di diversi dispositivi IoT indipendentemente dal tipo di connessione (diretta, basata su hub o). cloud-to-cloud

Le seguenti sono le funzionalità chiave relative a Matter:

- Dispositivo SDKs che supporta ZigBee i protocolli Z-Wave, Matter e Wi-Fi
- Oltre 80 modelli di modelli di dati dei dispositivi basati sull' AWS implementazione dello standard del modello di dati Matter
- Connettori sviluppati dai partner cloud-to-cloud (C2C)
- Controllo unificato dei dispositivi su più marchi e protocolli
- Disponibile nelle regioni di Canada (Centrale), Europa (Irlanda) e Medio Oriente (Emirati Arabi Uniti)

Per ulteriori informazioni, consulta A [cosa servono le integrazioni gestite?](#) AWS IoT Device Management

FAQs sullo standard Matter

Quali sono i livelli di iscrizione a Matter?

Le informazioni sull'iscrizione sono disponibili sul [sito web del CSA](#). Il livello di iscrizione scelto dipende dal vostro interesse a certificare un prodotto (adopter) o a definire il tipo di prodotto all'interno dello standard (partecipante). Per ulteriori informazioni sui livelli di iscrizione, consulta [Impact the Future of the IoT](#) sul sito Web CSA.

In che modo i consumatori di case intelligenti traggono vantaggio da Matter?

I consumatori traggono vantaggio da Matter nei seguenti modi:

- Onboarding semplificato dei dispositivi Matter a casa, incluso un flusso di configurazione avanzato, codici QR multidispositivo e onboarding NFC (versione 1.4.1 di Matter)
- Gestione unificata di tutti i dispositivi per la casa intelligente tramite un'unica app nei principali ecosistemi (Amazon Alexa, Google Home, Apple, Samsung) HomeKit SmartThings
- Controllo del dispositivo da più assistenti vocali contemporaneamente tramite Enhanced Multi-Admin (versione Matter 1.4)
- Accesso a diversi tipi di dispositivi, tra cui telecamere con streaming, elettrodomestici, dispositivi di gestione dell'energia e aspirapolvere robotici

Per ulteriori informazioni, consulta la sezione [Vantaggi della certificazione Matter per i consumatori di case intelligenti](#) in questa guida.

In che modo i produttori di dispositivi traggono vantaggio da Matter?

I produttori di dispositivi traggono vantaggio da Matter nei seguenti modi:

- Costi ridotti per supportare i clienti con problemi di infrastruttura e connettività
- Una singola certificazione per dispositivo anziché più certificazioni per ogni ecosistema

- Lo sviluppo di app proprietarie non è più necessario per le funzionalità di base del dispositivo
- Riduzione dei costi dei materiali grazie alla mancata spedizione di elementi dell'infrastruttura (come Thread Border Routers)
- Costi ridotti per supportare i clienti con problemi di infrastruttura e connettività
- Accesso a strumenti di sviluppo e infrastrutture di test maturi SDKs (notevolmente migliorato rispetto alla versione iniziale)
- Più rapido time-to-market grazie a processi di certificazione consolidati e reti ampliate di fornitori di test

Per ulteriori informazioni, consulta la sezione [Vantaggi della certificazione Matter per i produttori di dispositivi](#) in questa guida.

Matter sostituisce Wi-Fi, Bluetooth o Thread?

No, Matter è un protocollo a livello di applicazione che funziona su reti IP. I dispositivi che utilizzano Wi-Fi, Ethernet o Thread per la connettività possono ottenere la certificazione Matter. La tabella seguente riassume il contrasto di Matter con Wi-Fi, Bluetooth e Thread.

Funzionalità	Materia	Wi-Fi	Bluetooth	Thread
Scopo	Comunicazione Smart-home	Accesso a Internet e trasferimento dati	Comunicazione wireless a corto raggio	Rete mesh wireless a bassa potenza
Intervallo	Varia a seconda del protocollo sottostante	Fino a 300 piedi	Fino a 30 piedi	Fino a 300 piedi
Larghezza di banda	Varia a seconda del protocollo sottostante	Fino a 10 gigabit al secondo	Fino a 2 megabit al secondo	Fino a 250 kilobit al secondo
Consumo energetico	Varia a seconda del protocollo sottostante	Relativamente alto	Relativamente basso	Molto basso

Sicurezza	Varia a seconda del protocollo sottostante	WPA2, WPA3	Connessioni sicure AES, BLE	AES
Costo	Varia a seconda del dispositivo	Relativamente economico	Relativamente poco costoso	Relativamente costoso

Cosa sono l'ID del fornitore e l'ID del prodotto?

I membri CSA possono richiedere un ID fornitore che li identifichi come fornitore. I prodotti dell'azienda vengono d'ora in poi assegnati a questo ID e possono essere ricondotti alla loro origine. Inoltre, ricevono un ID prodotto univoco. Il codice numerico a 16 cifre accompagna i prodotti, come il numero del passaporto, e li rende inconfondibili tanto quanto il venditore.

Quali dispositivi devono essere certificati Matter?

Tutti i dispositivi che devono autenticarsi e far parte del tessuto Matter devono essere certificati Matter. Tuttavia, i dispositivi progettati per interagire solo con l'hub specificato dal fornitore tramite un protocollo non standard (proprietario) non trarrebbero vantaggio dal processo di certificazione Matter. Ad esempio, l'hub di un sistema di sicurezza domestica intelligente deve essere certificato come conforme a Matter, ma non è necessario che un sensore per porte o finestre che comunica con l'hub sia certificato come conforme a Matter. La scelta di ottenere la certificazione di un prodotto per Matter è guidata principalmente da questa considerazione.

Il mio tipo di prodotto non è attualmente definito in Matter. Per quali attività aggiuntive devo dedicare del tempo per ottenere la certificazione Matter dei prodotti?

Matter ha notevolmente ampliato la copertura dei tipi di dispositivi attraverso le versioni da 1.0 a 1.5. Lo standard ora supporta oltre 50 tipi di dispositivi, tra cui:

- Dispositivi principali: illuminazione, interruttori, prese, serrature, termostati, rivestimenti per finestre, sensori
- Elettrodomestici: frigoriferi, condizionatori d'aria, lavastoviglie, aspirapolvere robotici, microonde, forni

- **Gestione energetica:** pannelli solari, batterie, pompe di calore, scaldabagni, caricabatterie per veicoli elettrici
- **Ambientale:** dispositivi di gestione dell'acqua, sensori di qualità dell'aria, depuratori d'aria
- **Sicurezza:** telecamere con supporto per lo streaming

Se il tuo tipo di dispositivo non è ancora supportato, il primo passo è iscriverti al CSA come partecipante. Matter rilascia nuove versioni circa due volte all'anno, ampliando continuamente la copertura dei tipi di dispositivi. In qualità di membro partecipante, puoi guidare la definizione di nuovi tipi di dispositivi e avere accesso a bozze di specifiche che consentono una go-to-market strategia più rapida. Per ulteriori informazioni sui livelli di iscrizione, consulta [Impact the Future of the IoT](#) sul sito Web CSA.

Alcuni dei miei dispositivi si connettono direttamente alla rete Wi-Fi domestica. Questi dispositivi devono essere certificati Matter?

La certificazione Matter può avvantaggiare i dispositivi che si connettono direttamente alla rete smart-home perché possono connettersi alla struttura Matter. Ciò consente ai consumatori di controllare i dispositivi tramite i loro assistenti virtuali sullo stesso tessuto Matter. Tuttavia, i consumatori devono utilizzare un'app specifica per dispositivo per tutte le operazioni specifiche del fornitore e non definite nelle specifiche Matter.

Qual è la versione attuale di Matter e quali sono le novità?

A novembre 2025, Matter 1.5 è la versione attuale. Le principali aggiunte alle versioni recenti includono:

- **Matter 1.5 (novembre 2025):** supporto per lo streaming della fotocamera tramite RTSP, miglioramenti della stabilità
- **Matter 1.4.2 (giugno 2025):** messa in servizio BLE migliorata, crittografia basata su PSA, affidabilità del trasporto
- **Matter 1.4.1 (novembre 2024):** flusso di configurazione migliorato, codici QR multidispositivo, onboarding NFC
- **Matter 1.4 (novembre 2024):** Dispositivi di gestione dell'energia, Enhanced Multi-Admin, HRAP
- **Matter 1.3 (maggio 2024):** Elettrodomestici, caricabatterie per veicoli elettrici, rendicontazione energetica avanzata

- Matter 1.2 (ottobre 2023): frigoriferi, condizionatori d'aria, lavastoviglie, aspirapolvere robotici

Le versioni di Matter vengono rilasciate circa due volte all'anno dal gruppo di lavoro CSA.

Resources

AWS risorse

- [Ottieni il massimo da Matter con Alexa](#)
- [Annuncio del lancio di Matter e presentazione di Works with Alexa \(WWA\) for Matter per i dispositivi \(blog Amazon Alexa\)](#)

Connectivity Standards Alliance (CSA) per l'IoT

- [Sito web CSA](#)
- [Panoramica del processo di certificazione CSA](#)
- [Fornitori di test autorizzati CSA](#)
- [Specifiche della materia](#)

Cronologia dei documenti

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

Modifica	Descrizione	Data
Aggiornamenti alla versione standard di Matter	Aggiornato per includere informazioni sull'ultimo standard Matter, la versione 1.5	6 marzo 2026
Pubblicazione iniziale	—	5 febbraio 2024

AWS Glossario delle linee guida prescrittive

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

Numeri

7 R

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

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

A

A2A () Agent-to-Agent

Un protocollo statico per la collaborazione tra agenti che supporta la delega delle attività e il trasferimento dello stato.

ABAC

[Vedi controllo degli accessi basato sugli attributi.](#)

servizi astratti

Vedi [servizi gestiti](#).

ACIDO

Vedi [atomicità, consistenza, isolamento, durata](#).

migrazione attiva-attiva

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

migrazione attiva-passiva

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

Agente

Un sistema di intelligenza artificiale in grado di ragionare, pianificare e intraprendere azioni in modo autonomo utilizzando strumenti per raggiungere gli obiettivi.

Agente Ops

Pratiche operative per la creazione, il test, l'implementazione e l'esecuzione di agenti di intelligenza artificiale in produzione su larga scala.

funzione aggregata

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

Intelligenza artificiale

Vedi [intelligenza artificiale](#).

AIOps

Guarda le [operazioni di intelligenza artificiale](#).

anonimizzazione

Il processo di eliminazione permanente delle informazioni personali in un set di dati.

L'anonimizzazione può aiutare a proteggere la privacy personale. I dati anonimi non sono più considerati dati personali.

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

Il processo di utilizzo delle tecniche di machine learning per risolvere problemi operativi, ridurre gli incidenti operativi e l'intervento umano e aumentare la qualità del servizio. Per ulteriori

informazioni su come viene utilizzato AIOps nella strategia di migrazione AWS , consulta la [guida all'integrazione delle operazioni](#).

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

Un framework di linee guida e best practice AWS per aiutare le organizzazioni a sviluppare un piano efficiente ed efficace per passare con successo al cloud. AWS CAF organizza le linee guida in sei aree di interesse chiamate prospettive: business, persone, governance, piattaforma, sicurezza e operazioni. Le prospettive relative ad azienda, persone e governance si concentrano sulle competenze e sui processi aziendali; le prospettive relative alla piattaforma, alla sicurezza e alle operazioni si concentrano sulle competenze e sui processi tecnici. Ad esempio, la prospettiva relativa alle persone si rivolge alle parti interessate che gestiscono le risorse umane (HR), le funzioni del personale e la gestione del personale. In questa prospettiva, AWS CAF fornisce linee

guida per lo sviluppo delle persone, la formazione e le comunicazioni per aiutare a preparare l'organizzazione all'adozione del cloud di successo. Per ulteriori informazioni, consulta il [sito web di AWS CAF](#) e il [white paper AWS CAF](#).

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

Un [bot](#) che ha lo scopo di disturbare o causare danni a individui o organizzazioni.

BCP

Vedi la [pianificazione della continuità operativa](#).

grafico comportamentale

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

sistema big-endian

Un sistema che memorizza per primo il byte più importante. Vedi anche [endianness](#).

Classificazione binaria

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

filtro Bloom

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

blue/green dispiegamento

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

bot

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

botnet

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

ramo

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

accesso break-glass

In circostanze eccezionali e tramite una procedura approvata, un mezzo rapido per consentire a un utente di accedere a un sito a Account AWS cui in genere non dispone delle autorizzazioni necessarie. Per ulteriori informazioni, consulta l'indicatore [Implementare le procedure break-glass](#) nella guida. AWS Well-Architected

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

C

CAF

Vedi [AWS Cloud Adoption Framework](#).

implementazione canaria

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

CoE

Vedi [Cloud Center of Excellence](#).

CDC

Vedi [Change Data Capture](#).

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi [integrazione continua e distribuzione continua](#).

classificazione

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

Sviluppatore cittadino

Un utente aziendale che crea applicazioni di intelligenza artificiale utilizzando piattaforme senza code/low codice senza competenze tecniche specializzate.

crittografia lato client

Crittografia dei dati localmente, prima che il bersaglio li Servizio AWS riceva.

centro di eccellenza del cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

- Progetto: esecuzione di alcuni progetti relativi al cloud per scopi di dimostrazione e apprendimento
- Fondamento: effettuare investimenti fondamentali per dimensionare l'adozione del cloud (ad esempio, creazione di una zona di destinazione, definizione di un CCoE, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni
- Re-invention — 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 Enterprise Strategy. Cloud AWS Per informazioni sulla loro relazione con la strategia di AWS migrazione, consulta la guida alla [preparazione alla migrazione](#).

CMDB

Vedi [database di gestione della configurazione](#).

repository di codice

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

integrazione e distribuzione continue () CI/CD

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

CV

Vedi [visione artificiale](#).

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

Un processo per identificare e classificare i dati nella rete in base alla loro criticità e sensibilità. È un componente fondamentale di qualsiasi strategia di gestione dei rischi di sicurezza informatica

perché consente di determinare i controlli di protezione e conservazione appropriati per i dati. La classificazione dei dati è un componente del pilastro della sicurezza nel AWS Well-Architected Framework. Per ulteriori informazioni, consulta [Classificazione dei dati](#).

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di [definizione del database](#).

deep ensemble

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

deep learning

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

difesa in profondità

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

[Vedi ambiente.](#)

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

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

gemello digitale

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

tabella delle dimensioni

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

disastro

Un evento che impedisce a un carico di lavoro o a un sistema di raggiungere gli obiettivi aziendali nella sua sede principale di implementazione. Questi eventi possono essere disastri naturali,

guasti tecnici o il risultato di azioni umane, come errori di configurazione involontari o attacchi di malware.

disaster recovery (DR)

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

DML

Vedi linguaggio di [manipolazione del database](#).

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro *Domain-Driven Design: Tackling Complexity in the Heart of Software* (Boston: Addison-Wesley Professional, 2003). Per informazioni su come utilizzare la progettazione basata sul dominio con lo strangler fig pattern, consulta [Modernizzare i servizi Web Microsoft ASP.NET \(ASMX\) legacy in modo incrementale utilizzando contenitori e Amazon API Gateway](#).

DOTT.

Vedi [disaster recovery](#).

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, puoi utilizzarlo AWS CloudFormation per [rilevare la deriva nelle risorse di sistema](#) oppure puoi usarlo AWS Control Tower per [rilevare cambiamenti nella tua landing zone](#) che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la [mappatura del flusso di valore dello sviluppo](#).

E

EDA

Vedi [analisi esplorativa dei dati](#).

MODIFICA

Vedi [scambio elettronico di dati](#).

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. Big-endian i sistemi memorizzano per primi il byte più importante. Little-endian i sistemi memorizzano per primi il byte meno importante.

endpoint

Vedi [service endpoint](#).

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

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

epica

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

ERP

Vedi [pianificazione delle risorse aziendali](#).

analisi esplorativa dei dati (EDA)

Il processo di analisi di un set di dati per comprenderne le caratteristiche principali. Si raccolgono o si aggregano dati e quindi si eseguono indagini iniziali per trovare modelli, rilevare anomalie

e verificare ipotesi. L'EDA viene eseguita calcolando statistiche di riepilogo e creando visualizzazioni di dati.

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi [filiale](#).

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

Per ottimizzare i dati per il processo di machine learning, incluso l'arricchimento dei dati con fonti aggiuntive, il dimensionamento dei valori o l'estrazione di più set di informazioni da un singolo campo di dati. Ciò consente al modello di ML di trarre vantaggio dai dati. Ad esempio, se suddividi

la data "2021-05-27 00:15:37" in "2021", "maggio", "giovedì" e "15", puoi aiutare l'algoritmo di apprendimento ad apprendere modelli sfumati associati a diversi componenti dei dati.

prompt con pochi scatti

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

FGAC

Vedi il controllo [granulare degli accessi](#).

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

[Vedi il modello di base.](#)

modello di fondazione (FM)

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

Gateway FM

[Un intermediario centralizzato che controlla e normalizza l'accesso ai modelli di base.](#) Conosciuto anche come gateway LLM.

G

IA generativa

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

blocco geografico

Vedi [restrizioni geografiche](#).

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

Una regola di 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 CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector e controlli personalizzati AWS Lambda .

guardrail (AI)

Meccanismi di sicurezza che filtrano, convalidano e limitano gli input e gli output degli [agenti](#) per contribuire a garantire un comportamento dell'IA responsabile e sicuro.

H

AH

Vedi [disponibilità elevata](#).

migrazione di database eterogenea

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di esclusione

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

human-in-the-loop (HITL)

Un modello di flusso di lavoro in cui l'esecuzione degli [agenti](#) viene sospesa per la revisione e l'approvazione umana nei punti decisionali critici.

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

I

IaC

Vedi l'[infrastruttura come codice](#).

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi [Industrial Internet of Things](#).

infrastruttura immutabile

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

VPC in ingresso (ingresso)

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

migrazione incrementale

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

Internet delle cose industriale (IIoT)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi [Internet of Things](#).

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la [libreria di informazioni IT](#).

ITSM

Vedi [Gestione dei servizi IT](#).

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi [basato su etichette](#).

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi [7 R](#).

sistema little-endian

Un sistema che memorizza per primo il byte meno importante. Vedi anche [endianità](#).

LLM

Vedi modello [linguistico di grandi dimensioni](#).

ambienti inferiori

Vedi [ambiente](#).

M

machine learning (ML)

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

ramo principale

Vedi [filiale](#).

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi [Migration Acceleration Program](#).

MCP

Vedi [Model Context Protocol](#).

Model Context Protocol (MCP)

[Un protocollo stateless per la comunicazione tra agenti e strumenti](#).

Server MCP

Un servizio che espone uno o più [strumenti](#) tramite il [Model Context](#) Protocol.

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, vedete [Creazione di meccanismi](#) nel AWS Well-Architected Framework.

account membro

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

MEH

Vedi [sistema di esecuzione della produzione](#).

Message Queuing Telemetry Transport (MQTT)

[Un protocollo di comunicazione da macchina a macchina \(M2M\) leggero, basato sul publish/subscribe modello, per dispositivi IoT con risorse limitate.](#)

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

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

migrazione su larga scala

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

fabbrica di migrazione

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

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

[Vedi machine learning.](#)

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi [Migration Portfolio Assessment](#).

MQTT

Vedi [Message Queuing Telemetry Transport](#).

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi [Origin Access Control](#).

QUERCIA

Vedi [Origin Access Identity](#).

OCM

Vedi [gestione delle modifiche organizzative](#).

migrazione offline

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

OI

Vedi [l'integrazione delle operazioni](#).

OLA

Vedi accordo a [livello operativo](#).

migrazione online

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

OPC-UA

Vedi [Open Process Communications - Unified Architecture](#).

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

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

gestione del cambiamento organizzativo (OCM)

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

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

[Vedi la revisione della prontezza operativa.](#)

- NON

Vedi la [tecnologia operativa](#).

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le [informazioni di identificazione personale](#).

playbook

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

PLC

Vedi [controllore logico programmabile](#).

PLM

Vedi la gestione [del ciclo di vita del prodotto](#).

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

[Vedi ambiente.](#)

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

Vedi [responsabile, responsabile, consultato, informato \(RACI\)](#).

RAG

Vedi [Retrieval](#) Augmented Generation.

ransomware

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

Matrice RASCI

Vedi [responsabile, responsabile, consultato, informato \(RACI\)](#).

RCAC

Vedi controllo dell'[accesso a righe e colonne](#).

replica di lettura

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

riprogettare

Vedi [7 Rs](#).

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi [7 R.](#)

Region

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

regressione

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

riospitare

Vedi [7 R.](#)

rilascio

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

trasferisco

Vedi [7 Rs.](#)

ripiattaforma

Vedi [7 Rs.](#)

riacquisto

Vedi [7 Rs.](#)

resilienza

La capacità di un'applicazione di resistere o ripristinare le interruzioni. [L'elevata disponibilità e il disaster recovery](#) sono considerazioni comuni quando si pianifica la resilienza in Cloud AWS. [Per ulteriori informazioni, vedere Cloud AWS Resilience](#).

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi [7 R](#).

andare in pensione

Vedi [7 Rs](#).

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi [obiettivo del punto di ripristino](#).

VERSO

Vedi [obiettivo del tempo di ripristino](#).

runbook

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

S

SAML 2.0

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

SCADA

Vedi [controllo di supervisione e acquisizione dati](#).

SCP

Vedi la [politica di controllo del servizio](#).

Secret

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

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

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

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

[Una metrica target che rappresenta lo stato di un servizio, misurato da un indicatore del livello di servizio.](#)

Modello di responsabilità condivisa

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

Shadow AI

Applicazioni di [intelligenza artificiale](#) non autorizzate create o utilizzate al di fuori dei canali regolamentati all'interno di un'organizzazione.

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](#).

modello split-and-seed

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 [Modernizzare i servizi Web Microsoft ASP.NET \(ASMX\) legacy in modo incrementale utilizzando contenitori e Amazon API Gateway](#).

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

T

tag

Key-value coppie 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.

strumento

Una funzione o API che un [agente](#) può richiamare per eseguire operazioni in sistemi esterni.

Transit Gateway

Un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti on-premise. Per ulteriori informazioni, consulta [Cos'è un gateway di transito](#) nella AWS Transit Gateway documentazione.

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

U

incertezza

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

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.

prompt zero-shot

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

applicazione zombie

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

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