



Patching automatizzato per istanze mutabili nel cloud ibrido utilizzando AWS Systems Manager

# AWS Guida prescrittiva



# AWS Guida prescrittiva: Patching automatizzato per istanze mutabili nel cloud ibrido utilizzando AWS Systems Manager

Copyright © 2024 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 delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

---

# Table of Contents

Introduzione .....	1
Panoramica .....	3
Termini e concetti .....	4
Storie chiave degli utenti .....	5
Processo di patch .....	8
Progettazione di istanze EC2 mutabili .....	10
Processo automatizzato .....	10
Progettazione per piùAWSaccount e regioni .....	13
Processo automatizzato .....	13
Considerazioni e limitazioni relative all'architettura .....	14
Quote della finestra di manutenzione per conto .....	14
Altre considerazioni .....	15
Progettazione per istanze on-premise in ambiente cloud ibrido .....	16
Processo automatizzato .....	16
Considerazioni e limitazioni relative all'architettura .....	18
Stakeholder chiave, ruoli e responsabilità .....	20
Personaggi utente .....	20
Matrice RACI .....	21
Fasi successive .....	25
Risorse aggiuntive .....	26
Cronologia dei documenti .....	27
Glossario .....	28
# .....	28
A .....	29
B .....	32
C .....	34
D .....	37
E .....	41
F .....	43
G .....	45
H .....	45
I .....	47
L .....	49
M .....	50

---

O .....	55
P .....	57
Q .....	60
R .....	60
S .....	63
T .....	67
U .....	68
V .....	69
W .....	69
Z .....	71
.....	lxxii

# Patching automatizzato per istanze mutabili nel cloud ibrido utilizzando AWS Systems Manager

Chandra Allaka, Amazon Web Services (AWS)

Giugno 2020([cronologia dei documenti](#))

Questa guida prescrittiva descrive una soluzione di patch automatizzata che utilizza Amazon Web Services (AWS) Systems Manager. Puoi utilizzare questa soluzione per patch per patch su istanze Amazon AWS Account e AWS Regioni e istanze locali.

Questa guida è destinata agli utenti che sono coinvolti nella progettazione e nello sviluppo di funzionalità operative in un ambiente cloud ibrido per consentire ai team applicativi di rispettare le policy sulle patch aziendali. Fornisce un meccanismo self-service per distribuire patch preapprovate sui server delle applicazioni.

Questa guida presuppone una buona comprensione di quanto segue AWS servizi e concetti:

- [Systems Manager](#)— Fornisce un'interfaccia utente unificata per la visualizzazione dei dati operativi da più AWS servizi e automazione delle attività operative in tutti i AWS risorse.
- [Inventario Systems Manager](#)— Fornisce visibilità su Amazon EC2 e sull'ambiente di elaborazione locale. Puoi utilizzare Inventory per raccogliere i metadati dalle tue istanze gestite.
- [Patch Manager di Systems Manager](#)— Automatizza il processo di patch alle istanze gestite con aggiornamenti.
- [Systems Manager e manutenzione Windows](#)— Consente di definire una pianificazione per l'esecuzione di operazioni potenzialmente problematiche sulle istanze, ad esempio l'applicazione di patch al sistema operativo, l'aggiornamento di driver o l'installazione di software o patch.
- [AWS Lambda](#) - Consente di eseguire il codice senza effettuare il provisioning dei server o senza gestirli.
- [Amazon QuickSight](#)— Consente di creare e pubblicare facilmente dashboard interattivi, inclusi approfondimenti sull'apprendimento automatico (ML). Puoi accedere alle dashboard da qualsiasi dispositivo e incorporarle nelle tue applicazioni, portali e siti Web.

- [Applicazione di tag](#)— Consente di assegnare i metadati alAWSrisorse di sotto forma di tag. Ogni tag è un'etichetta composta da una chiave e da un valore definiti dall'utente. Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse.

# Panoramica della gestione delle patch

Se siete coinvolti in operazioni di applicazioni o infrastrutture, comprendete l'importanza di una soluzione di patch del sistema operativo (OS) sufficientemente flessibile e scalabile da soddisfare i diversi requisiti dei team applicativi. In un'organizzazione tipica, alcuni team applicativi utilizzano un'architettura che coinvolge istanze immutabili mentre altri distribuiscono le loro applicazioni su istanze mutabili.

L'applicazione di patch alle istanze immutabili implica l'applicazione delle patch alle Amazon Machine Images (AMI) utilizzate per fornire le istanze immutabili dell'applicazione EC2. L'applicazione di patch alle istanze mutabili implica la distribuzione di patch in loco alle istanze in esecuzione durante una finestra di manutenzione pianificata.

Questa guida prescrittiva descrive come utilizzare AWS Systems Manager Patch Manager per applicare patch a istanze mutabili che si estendono su più AWS account e AWS regioni in modo automatico, in base alle finestre di manutenzione e ai gruppi di patch definiti dai team dell'applicazione sui propri server tramite tag.

La guida descrive una soluzione di patch automatizzata che consente di automatizzare le configurazioni e la pianificazione delle patch, utilizzando Patch Manager e finestre di manutenzione. Amazon QuickSight offre le funzionalità di reporting e dashboard necessarie per segnalare la conformità delle patch.

Inoltre, questa guida descrive un'architettura di riferimento per ambienti cloud ibridi. Gli utenti che eseguono le proprie applicazioni in una configurazione cloud ibrida cercano opportunità per consolidare, semplificare, standardizzare e ottimizzare le operazioni di gestione delle patch all'interno dell'infrastruttura locale. La guida spiega come la soluzione di patch automatizzata per istanze mutabili può essere estesa per supportare scenari di cloud ibrido.

Questa guida descrive:

- Storie chiave degli utenti per la gestione delle patch
- Il processo di patching
- Gestione delle patch per istanze mutabili in un unico account e in un'unica AWS regione; considerazioni e limitazioni architetturiche
- Gestione delle patch per istanze mutabili in un ambiente con più account e più regioni; considerazioni e limitazioni architetturiche

- Gestione delle patch per istanze locali in un ambiente cloud ibrido; considerazioni e limitazioni architettoniche
- Principali stakeholder, ruoli e responsabilità

### Note

Questa guida descrive un'architettura per una soluzione automatizzata (denominata soluzione di patching automatizzata) che è possibile implementare per supportare i requisiti di gestione delle patch per le istanze mutabili. Non fornisce il codice per creare la soluzione.

## Termini e concetti

Termine	Definizione
Istanze immutabili	Le istanze immutabili sono istanze del server EC2 che non subiscono alcuna modifica durante l'esecuzione. Se sono necessarie modifiche, si crea una nuova istanza con l'immagine del server aggiornata, si ridistribuisce l'istanza e si distrugge l'immagine del server esistente.
Linea di base delle patch	Una patch di base è specifica per un tipo di sistema operativo e definisce l'elenco delle patch approvate per l'installazione sulle istanze. Per ulteriori informazioni, vedere <a href="#">Informazioni sulle baseline delle patch predefinite e personalizzate</a> nella documentazione di Systems Manager.
Gruppo di patch	Un gruppo di patch rappresenta i server all'interno di un ambiente applicativo che sono obiettivi di una specifica baseline di patch. I gruppi di patch garantiscono che le basi di patch corrette siano distribuite al set di istanze



Termine	Definizione
	<p>corretto. Inoltre aiutano a evitare l'installazione di patch prima che siano state adeguatamente testate. I gruppi di patch sono rappresentati dal tag Patch Group. Per ulteriori informazioni, vedere Informazioni <a href="#">sui gruppi di patch</a> nella documentazione di Systems Manager.</p>
Maintenance window (Finestra di manutenzione)	<p>Le finestre di manutenzione consentono di definire una pianificazione dei periodi in cui eseguire operazioni potenzialmente problematiche sulle istanze, ad esempio l'applicazione di patch al sistema operativo, l'aggiornamento di driver o l'installazione di software o patch. Ogni finestra di manutenzione include una pianificazione, una durata massima, un set di istanze target registrate e un set di attività registrate. Le finestre di manutenzione sono rappresentate dal tag Maintenance Window. Per ulteriori informazioni, vedere <a href="#">Informazioni sulla pianificazione delle patch utilizzando le finestre di manutenzione</a> nella documentazione di Systems Manager.</p>

## Storie chiave degli utenti

Il tipico processo di patching del sistema operativo prevede tre attività:

1. Scansione delle istanze EC2 e dei server locali alla ricerca di patch del sistema operativo applicabili.
2. Raggruppamento e applicazione delle patch alle istanze in un momento opportuno.
3. Segnalazione della conformità delle patch in tutto l'ambiente server.

La tabella seguente seguente seguente seguente seguente seguente seguente seguente seguente seguente seguente seguente seguente seguente.

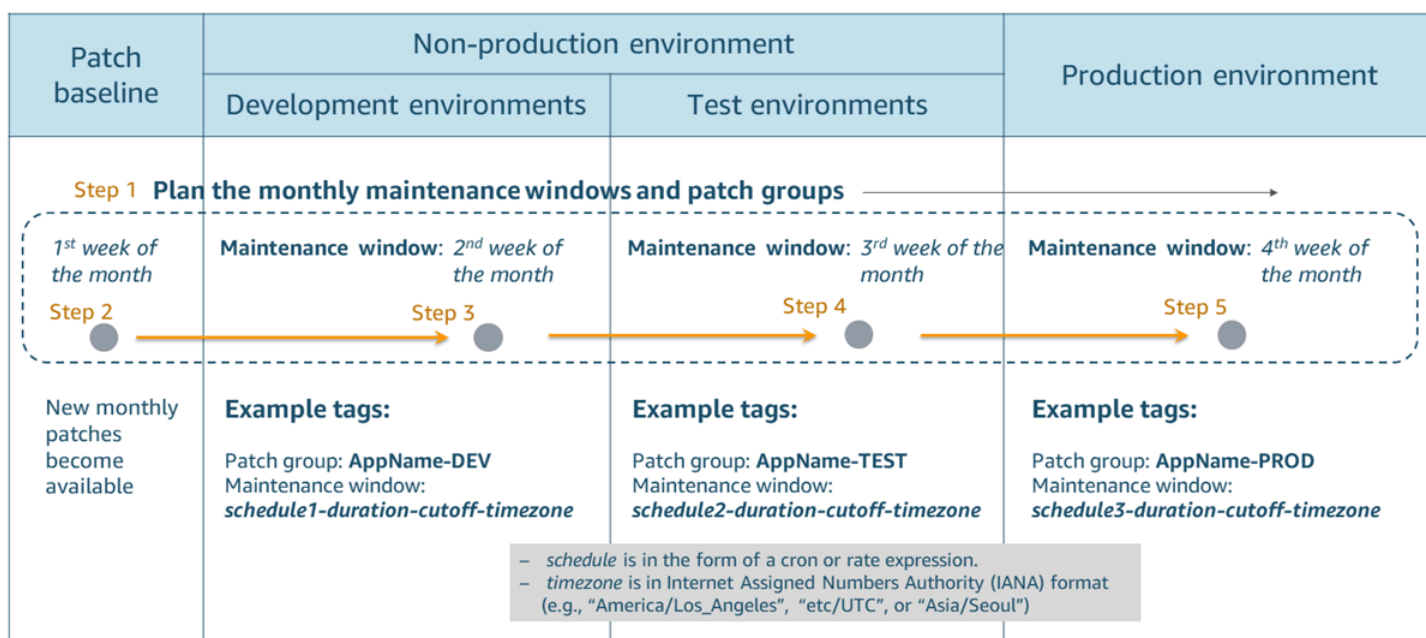
Scenario	Ruolo dell'utente	Descrizione
Meccanismo di riparazione	Team di sviluppo/supporto delle applicazioni	In qualità di membro del team applicativo responsabile dell'applicazione delle patch del sistema operativo, ho bisogno di un meccanismo per correggere le mie istanze modificabili o in esecuzione da lungo tempo, in modo da poter mitigare eventuali vulnerabilità di sicurezza del sistema operativo e garantire anche che le istanze siano conformi alla linea di base di patch definita dal team di sicurezza.
Soluzione di patching	Proprietario del servizio cloud	In qualità di proprietario di servizi cloud responsabile della fornitura di servizi cloud ai team applicativi, devo creare una soluzione di patch del sistema operativo che supporti piùAWS account eAWS regioni, nonché server locali, in modo che i team applicativi possano mitigare eventuali vulnerabilità di sicurezza del sistema operativo e rimanere conformi alla linea di base per l'applicazione delle patch definita dal team di sicurezza.
Rapporti di conformità relativi alle patch	Responsabile delle operazioni di sicurezza	In qualità di responsabile delle operazioni di sicurezza

Scenario	Ruolo dell'utente	Descrizione
		responsabile della conformità delle patch, ho bisogno di report e informazioni dettagliati sulla conformità delle patch in tutto il panorama cloud, in modo da poter identificare i server che non sono conformi alla linea di base delle patch e avvisare i team per implementare la mitigazione richiesta.
Definizione di ruoli e responsabilità	Proprietario del servizio cloud	In qualità di proprietario di un servizio cloud, devo creare una matrice di ruoli e responsabilità ben definita che spieghi chi fa cosa nella gestione della soluzione di patching sul cloud ibrido che ho creato, in modo che gli obblighi relativi alle operazioni di patch siano pubblicati e rispettati.

# Processo di patch

Gli utenti principali della soluzione di patch sono i team di sviluppo delle applicazioni e operazioni. Ogni applicazione viene in genere distribuita in più ambienti, come sviluppo, test (integrazione, accettazione degli utenti e così via) e produzione. I team applicativi devono pianificare i programmi di patch per ciascun ambiente, quindi quando una patch viene applicata all'ambiente di produzione, è già stata testata e determinata di non avere effetti negativi sull'applicazione.

Il flusso di lavoro seguente fornisce un esempio di come pianificare le finestre di patch per un'applicazione distribuita in più ambienti e come configurare i tag.



- Fase 1: Ogni team di applicazioni pianifica le finestre di manutenzione per i server in diversi ambienti e imposta di conseguenza i tag che rappresentano i gruppi di patch e le finestre di manutenzione dei server:
  - LaGruppo di patchtag rappresenta i server all'interno di un ambiente applicativo che sono gli obiettivi di una specifica baseline di patch. I gruppi di patch garantiscono che vengano distribuite le basi di patch corrette. Inoltre aiutano a non distribuire le patch non adeguatamente verificate.
  - Se gli application server includono più sistemi operativi, il team applicativo crea gruppi di patch basati sulla combinazione di ambiente e sistema operativo. Un gruppo di patch può essere registrato con una sola baseline di patch e un'istanza può far parte di un solo gruppo di patch.

Ad esempio: *appname*-DEV-WINE*appname*-DEV-RHEL

- La Finestra di manutenzione tag rappresenta la pianificazione per l'applicazione di patch ai server. Tutti i server di un gruppo di patch devono trovarsi nella stessa finestra di manutenzione. Il tag della finestra di manutenzione deve seguire un formato coerente per le espressioni cron e rate in modo che una funzione Lambda definita possa analizzare facilmente le espressioni. (In questa guida, faremo riferimento a questa funzione Lambda come `automate-patch`.)

Ad esempio: *`schedule-duration-cutoff-timezone`*

`cron(0 2 ? * SAT#3 *)` rappresenta le 02.00 del terzo sabato di ogni mese. Per informazioni dettagliate sulle espressioni cron e rate, consulta [Documentazione di Systems Manager](#).

- Fase 2. Systems Manager Patch Manager rende disponibili regolarmente nuove patch tramite le baseline di patch specifiche del sistema operativo in base alle configurazioni definite.
  - Per ogni sistema operativo, è possibile definire una baseline di patch personalizzata che include le regole di approvazione e le patch che devono essere applicate alle istanze nell'ambiente cloud.
- Fase 3. Il codice di automazione personalizzato configura Patch Manager per configurare le patch in base al Gruppo di patch Finestra di manutenzione tag e applica le patch all'ambiente di sviluppo.
  - Una volta completata la patch, i team di sviluppo e supporto dell'applicazione testano l'applicazione e verificano che tutto funzioni correttamente.
  - Se l'applicazione incontra problemi con la nuova patch, i team di applicazioni chiedono al team dei servizi cloud di interrompere l'applicazione di patch ad altri gruppi di patch e altri ambienti, disabilitando le finestre di manutenzione o annullando la registrazione dell'esecuzione delle attività di patch.
- Fase 4. Dopo che l'ambiente di sviluppo è stato applicato correttamente, l'applicazione di patch viene distribuita in qualsiasi altro ambiente non di produzione. Come per l'ambiente di sviluppo, l'applicazione viene testata e verificata per funzionare correttamente in tutti gli ambienti non di produzione. In caso di problemi, i team applicativi chiedono al team dei servizi cloud di interrompere l'applicazione di patch all'ambiente di produzione.
- Fase 5: Dopo che tutti gli ambienti non di produzione sono stati sottoposti a patch, la patch viene applicata all'ambiente di produzione.

# Progettazione di soluzioni di patch per istanze EC2 mutabili

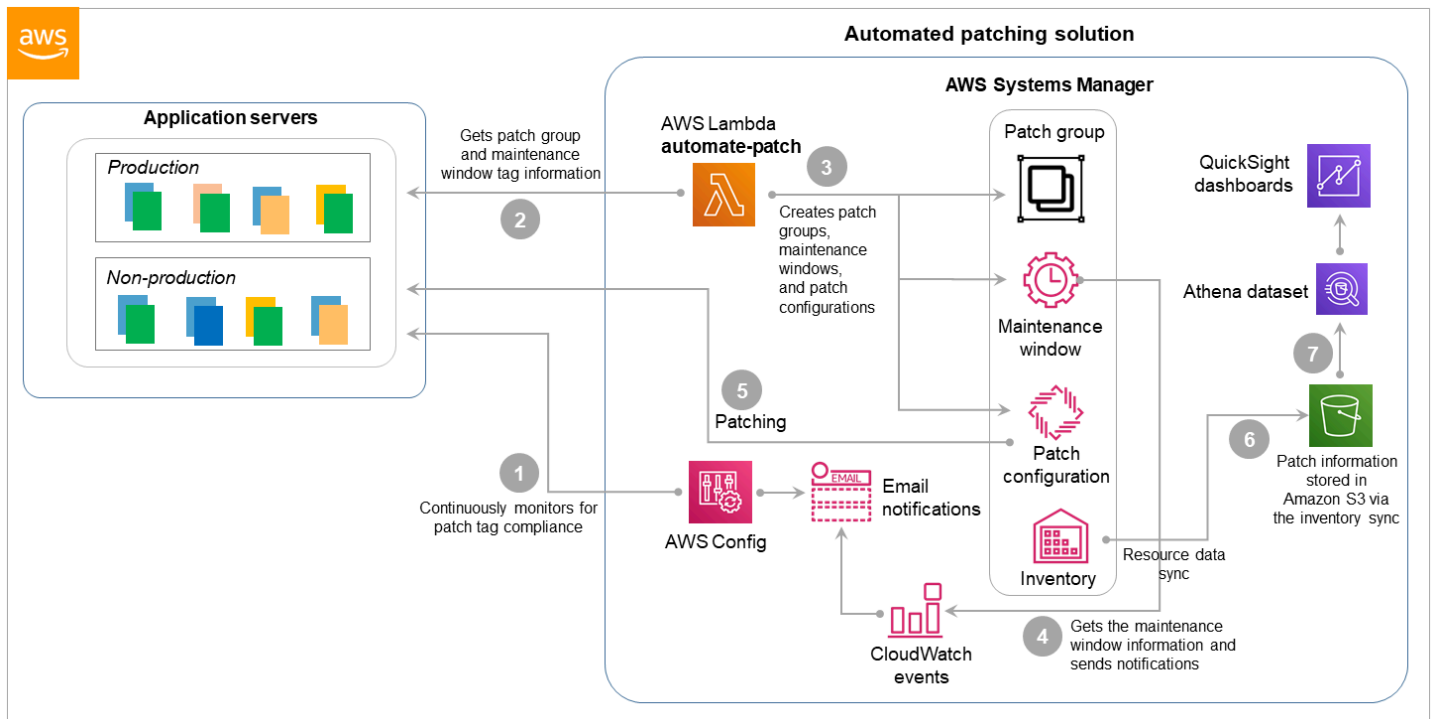
Il processo di patch per istanze mutabili coinvolge i seguenti team e azioni:

- I team applicativi (DevOps) definiscono i gruppi di patch per i server in base all'ambiente applicativo, al tipo di sistema operativo o ad altri criteri. Definiscono inoltre le finestre di manutenzione specifiche per ciascun gruppo di patch. Queste informazioni sono memorizzate sul Gruppo di patch Finestra di manutenzione tag delle istanze dell'applicazione EC2. Durante ogni ciclo di patch, i team dell'applicazione si preparano per l'applicazione di patch, testano l'applicazione dopo l'applicazione di patch e risolvono eventuali problemi relativi alle applicazioni e al sistema operativo durante l'applicazione di patch.
- I team di sicurezza definiscono le baseline delle patch per vari tipi di sistema operativo utilizzati dai team applicativi, approvano le patch e rendono disponibili le patch tramite Systems Manager Patch Manager.
- La soluzione di patch automatizzata viene eseguita regolarmente e distribuisce le patch definite nelle baseline delle patch in base ai gruppi di patch definiti dall'utente e alle finestre di manutenzione. Le informazioni sulla conformità delle patch vengono ottenute tramite una sincronizzazione dei dati delle risorse in Systems Manager Inventory e vengono utilizzate per il reporting sulla conformità delle patch tramite dashboard di Amazon QuickSight.
- I team di governance e conformità definiscono le linee guida sulle patch, definiscono i processi e i meccanismi delle eccezioni e ottengono la segnalazione di conformità da Amazon QuickSight.

Per informazioni dettagliate sulle principali parti interessate coinvolte in una soluzione di gestione delle patch del sistema operativo di successo e sulle loro responsabilità, vedere [il Stakeholder chiave, ruoli e responsabilità](#) più avanti in questa guida.

## Processo automatizzato

La soluzione di patch automatizzata utilizza molteplici AWS servizi che funzionano in tandem per distribuire le patch alle istanze EC2. Questo processo comporta AWS Config, AWS Lambda, Systems Manager, Amazon Simple Storage Service (Amazon S3) e Amazon QuickSight. Il diagramma seguente illustra l'architettura di riferimento e il flusso di lavoro.



Il flusso di lavoro include questi passaggi, in cui i numeri di fase corrispondono alle didascalie nel diagramma:

1. AWS Config monitora continuamente per quanto segue e invia notifiche con i dettagli delle istanze non conformi e le configurazioni necessarie:
  - Conformità alle patch tagging sulle istanze EC2. AWS Config controlla le istanze che non hanno Gruppo di patche Finestra di manutenzione tag.
  - La AWS Identity and Access Management (IAM) profilo di istanza con il ruolo di Systems Manager, che consente a Systems Manager di gestire le istanze.
2. La funzione Lambda (la chiameremo `automate-patch`) viene eseguito su una pianificazione predefinita e raccoglie il Gruppo di patche Finestra di manutenzione informazioni per tutti i server.
3. La `automate-patch` funzione quindi crea o aggiorna i gruppi di patch e le finestre di manutenzione appropriati, associa i gruppi di patch alle baseline delle patch, configura la scansione delle patch e distribuisce l'attività di patch. Facoltativamente, il `automate-patch` funzione crea anche eventi in Amazon CloudWatch Events per notificare agli utenti le patch imminenti.
4. In base alle finestre di manutenzione, gli eventi inviano notifiche di patch ai team dell'applicazione con i dettagli dell'imminente operazione di patch.
5. Patch Manager esegue patch di sistema in base alla pianificazione definita e ai gruppi di patch.

6. Una sincronizzazione dei dati delle risorse in Systems Manager Inventory raccoglie i dettagli delle patch e li pubblica in un bucket S3.
7. I dashboard e i report sulla conformità delle patch sono integrati in Amazon QuickSight dalle informazioni sul bucket S3.

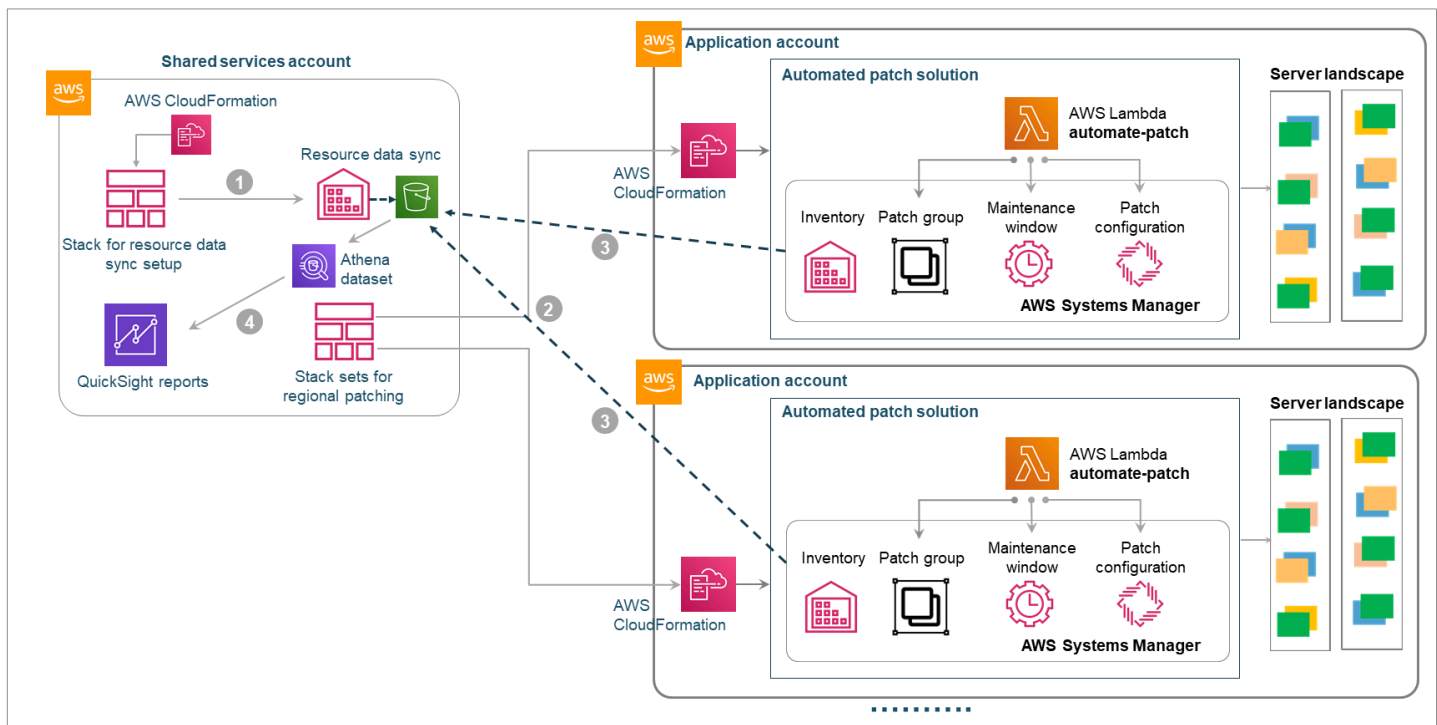


# Progettazione di soluzioni di patch per piùAWSAccount e regioni

È possibile estendere la soluzione di patch automatizzata per supportare server che si estendono su piùAWSAccount e multipliAWSRegioni. La soluzione estesa prevede l'impostazione della soluzione di automazione delle patch in ciascunaAWSAccount tramiteAWS CloudFormationStackSets in un account di servizi condivisi e la configurazione di una sincronizzazione dei dati delle risorse tra gli account con l'account Shared Services.

## Processo automatizzato

Nel diagramma seguente viene illustrata l'architettura per questo scenario. Questa architettura includeAWS CloudFormationStackSets e unAWSAccount di servizio condiviso.



Il flusso di lavoro è simile al processo descritto nella sezione precedente, ma prevede i seguenti passaggi aggiuntivi, in cui i numeri di fase corrispondono alle didascalie nel diagramma:

1. Nell'account Shared Services, un'AWS CloudFormation stack Set viene utilizzato per configurare il bucket S3 per la sincronizzazione dei dati delle risorse tramite Systems Manager Inventory.

2. Il set di stack CloudFormation crea lo stack con `automate-patch` Funzione Lambda, imposta le baseline delle patch e imposta la sincronizzazione dei dati delle risorse di Systems Manager Inventory sugli account dell'applicazione, per sincronizzare le risorse nell'account di servizi condivisi.
3. Le informazioni sulle risorse negli account dell'applicazione vengono sincronizzate con le informazioni sulla risorsa nell'account di servizi condivisi.
4. Amazon QuickSight genera report sulla conformità delle patch, utilizzando il set di dati Amazon Athena per le informazioni sulle risorse sincronizzate.

## Considerazioni e limitazioni relative all'architettura

### Quote della finestra di manutenzione per conto

L'architettura illustrata e descritta nella sezione precedente crea una finestra di manutenzione per ciascun gruppo di patch. Tuttavia, la quota per il numero di finestre di manutenzione per `AWSaccount` è 50 (supponendo che non abbia richiesto un aumento della quota di servizio). Se si prevede che il numero di gruppi di patch superi 50 gruppi in un singolo `AWSaccount`, questa architettura non sarà scalabile per soddisfare le tue esigenze.

Se un aumento della quota di servizio non è sufficiente per le tue esigenze, ci sono due opzioni per gestire questa sfida: l'utilizzo di finestre di manutenzione predefinite e l'utilizzo di CloudWatch Events. Ecco i vantaggi e gli svantaggi di ogni approccio.

#### Opzione 1. Uso delle finestre di manutenzione predefinite

- Definire un elenco di finestre di manutenzione con diverse finestre temporali (ad esempio, da 15 a 20 finestre di manutenzione per account).
- I team applicativi scelgono le finestre di manutenzione più adatte a loro dall'elenco predefinito e contrassegnano le istanze di conseguenza.
- Aggiorna la soluzione di patch automatizzata per mappare i gruppi di patch alle finestre di manutenzione selezionate invece di creare nuove finestre di manutenzione.

pro:

- Gestione semplificata.

## Contro:

- Minore flessibilità per la definizione di finestre di manutenzione personalizzate.
- Quando più gruppi di patch condividono finestre di manutenzione e attività di patch, l'annullamento di un'attività di patch specifica per un gruppo di patch specifico richiede ulteriore sforzo manuale.

## Opzione 2. Usa CloudWatch Events per attivare attività di patch anziché utilizzare le finestre di manutenzione

- Invece di creare finestre di manutenzione, utilizza CloudWatch Events per attivare le attività di patch in base alla pianificazione e ai gruppi di patch.
- In questo scenario, ogni gruppo di patch è associato a un evento CloudWatch Events anziché a una finestra di manutenzione.
- Aggiorna la soluzione di patch automatizzata per creare eventi anziché finestre di manutenzione.

## pro:

- Design scalabile.
- Offre flessibilità per la definizione di finestre di manutenzione personalizzate.

## Contro:

- Le finestre di manutenzione forniscono funzionalità aggiuntive (come durata e tempi limite) che non sono disponibili con CloudWatch Events.

## Altre considerazioni

- La soluzione di patch automatizzata descritta in questa sezione non supporta le istanze EC2 che vengono chiuse.
- Questo processo supporta le istanze EC2 nelle sottoreti pubbliche. Per applicare patch alle istanze in subnet private, è necessario distribuire un [repository di patch locale come Windows Server Update Services \(WSUS\)](#).
- È necessario regolare la frequenza per l'esecuzione della funzione Lambda in modo che i gruppi di patch e le finestre di manutenzione vengano aggiornati in base alla pianificazione richiesta.

# Progettazione di soluzioni di patch per istanze on-premise in un ambiente cloud ibrido

È inoltre possibile estendere la soluzione descritta in questa guida per applicare patch alle istanze server locali in un ambiente cloud ibrido.

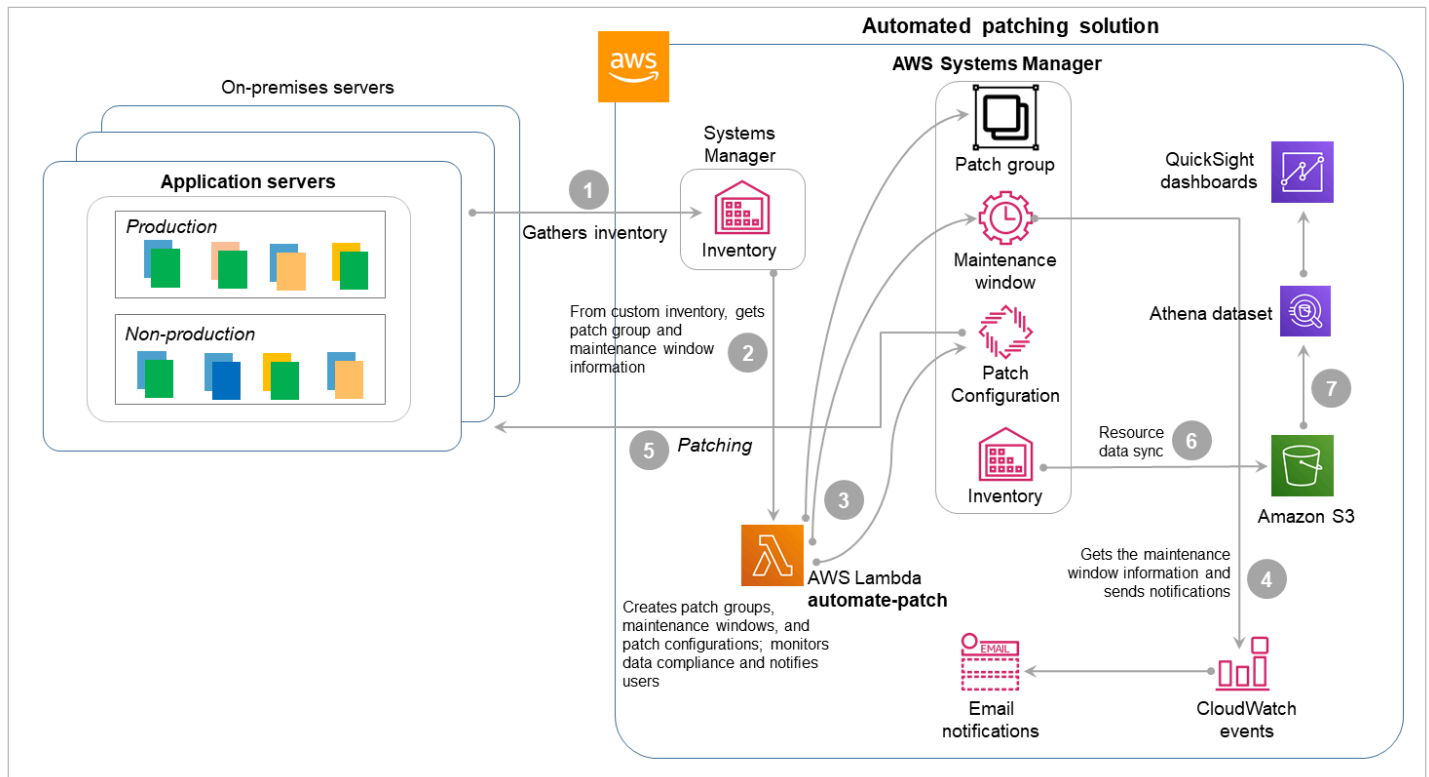
Il processo di patch standard per le istanze locali consiste in due fasi:

- È possibile configurare i server locali per essere gestiti da Systems Manager. Per informazioni dettagliate su questo processo, consulta [Configurazione di Systems Manager per ambienti ibridi](#) nella documentazione di Systems Manager.
- È possibile configurare l'appropriato Gruppo di patche Finestra di manutenzione tag per queste istanze gestite locali utilizzando il AWS Command Line Interface (AWS CLI) [comando add-tags-to-resource](#).

Tuttavia, questo approccio richiede che il team applicativo o il team cloud eseguano manualmente il AWS CLI comandi ogni volta che vogliono apportare modifiche ai gruppi di patch o alle finestre di manutenzione.

## Processo automatizzato

Nella figura seguente viene descritto un approccio alternativo alla patch delle istanze locali che utilizza l'opzione di inventario personalizzato di Systems Manager. Questo processo è un'estensione della soluzione di patch automatizzata descritta in precedenza per le istanze EC2 mutabili.



1. Invece di utilizzare i tag, Systems Manager acquisisce le informazioni sulle patch (gruppi di patch e finestre di manutenzione) dalle istanze gestite locali tramite una raccolta di inventario personalizzata.

Sample custom inventory JSON file

```
{
  "SchemaVersion": "1.0",
  "TypeName": "Custom:PatchInformation",
  "Content": {
    "Patch Group": "<APP-PROD>",
    "Maintenance Window": "XXX"
  }
}
```

2. La Lambda `automate-patch` funzione viene eseguita ogni giorno, raccoglie il gruppo di patch e le informazioni della finestra di manutenzione dall'inventario personalizzato del server locale e crea il Gruppo di patche Finestra di manutenzione tag sulle istanze gestite.
3. La Lambda `automate-patch` quindi crea o aggiorna i gruppi di patch e le finestre di manutenzione appropriati, associa i gruppi di patch alle baseline delle patch, configura le scansioni delle patch e distribuisce l'attività di patch, in base all'inventario personalizzato raccolto. Facoltativamente,

il `automate-patch` funzione crea anche eventi in CloudWatch Events per notificare agli utenti le patch imminenti.

4. In base alle finestre di manutenzione, gli eventi inviano notifiche di patch ai team dell'applicazione con i dettagli dell'imminente operazione di patch.
5. Patch Manager esegue patch di sistema in base alla pianificazione definita e ai gruppi di patch.
6. Una sincronizzazione dei dati delle risorse in Systems Manager Inventory raccoglie i dettagli delle patch e li pubblica in un bucket S3.
7. I dashboard e i report sulla conformità delle patch sono integrati in Amazon QuickSight dalle informazioni sul bucket S3.

## Considerazioni e limitazioni relative all'architettura

Come discusso nelle sezioni precedenti, esistono due approcci per applicare patch alle istanze locali: attraverso l'inventario personalizzato o utilizzando i tag. Ecco i vantaggi e gli svantaggi di ciascun approccio.

### Opzione 1. Usa l'inventario personalizzato per le informazioni sulle patch

- I team di applicazioni che lavorano con i server locali configurano le informazioni sulle patch nel modello di caricamento dati personalizzato e Systems Manager sceglie tali informazioni.
- Le informazioni personalizzate sulla patch dell'inventario vengono quindi utilizzate per creare le attività di patch.

pro:

- Molto più semplice da configurare perché comporta solo un aggiornamento dei file.

Contro:

- Le modifiche alla configurazione delle patch sono limitate al programma di raccolta dell'inventario.

### Opzione 2. Utilizzo dei tag per istanze locali

- Creano team di applicazioni che lavorano con i server locali Gruppo di patch Finestra di manutenzione tag utilizzando AWS CLI con le informazioni sulla patch appropriate.

- Le informazioni sui tag vengono utilizzate per creare le attività di patch.

pro:

- Approccio coerente AWS e on premise per favorire la standardizzazione e l'automazione delle patch.

Contro:

- I team applicativi che lavorano con istanze locali devono apprendere e utilizzare AWS CLI per creare o aggiornare i tag.

# Le principali parti interessate, ruoli e responsabilità nella gestione delle patch

La gestione efficace delle patch del sistema operativo richiede ruoli e responsabilità ben definiti per supportare la soluzione di patch automatizzata e ottimizzarla continuamente. Questa sezione descrive i ruoli e le responsabilità suggeriti che è possibile modificare in base alle proprie esigenze e alla struttura organizzativa.

## Personaggi utente

Nella tabella seguente vengono descritti i personaggi dell'utente coinvolti nella soluzione di patch automatizzata.

Persona utente	Descrizione
Consumatori (C)	<p>La soluzione di gestione delle patch per istanze di lunga durata viene utilizzata da diversi team coinvolti nella gestione del sistema operativo, tra cui:</p> <ul style="list-style-type: none"> <li>• Team di sviluppo che gestiscono ambienti applicativi full-stack.</li> <li>• Team operativi che gestiscono il sistema operativo del server applicazioni.</li> </ul>
Ingegneria cloud (CE)	<p>Il team responsabile di:</p> <ul style="list-style-type: none"> <li>• Ottimizzazione continua della soluzione di gestione delle patch.</li> <li>• Creazione di automazione dei servizi cloud.</li> <li>• Supporto dell'automazione.</li> </ul>
Ufficio aziendale cloud (CBO)	<p>Il team che è coinvolto in:</p> <ul style="list-style-type: none"> <li>• Gestire l'esperienza del consumatore per la soluzione.</li> </ul>



Persona utente	Descrizione
	<ul style="list-style-type: none"> <li>• Abilitazione e coinvolgimento degli utenti.</li> <li>• Assicurarsi che la soluzione patch soddisfi le esigenze dei consumatori.</li> </ul>
CPO (Cloud Service/product owner)	<p>La persona responsabile di:</p> <ul style="list-style-type: none"> <li>• Fornire servizi cloud ai consumatori.</li> <li>• Lavorare a stretto contatto con il team di leadership per allineare la fornitura di servizi alle aspettative e alle linee guida.</li> <li>• Gestire tutte le aspettative e le escalation dei clienti relative alla piattaforma.</li> <li>• Possedere la roadmap della piattaforma.</li> </ul>
Operazioni di sicurezza (SO)	Il team che gestisce le linee di base e le approvazioni delle patch.
Responsabile delle operazioni di sicurezza (SOM)	Il manager responsabile della conformità alle patch.

## Matrice RACI

La seguente matrice responsabile, responsabile, consultata, informata (RACI) specifica le attività coinvolte con la soluzione di gestione delle patch. Per ogni fase del processo, elenca gli stakeholder e il loro coinvolgimento:

- R— responsabile del completamento della fase
- UN— responsabile dell'approvazione e della firma del lavoro
- C— consultato per fornire input per un'attività
- I— informato dei progressi, ma non direttamente coinvolti nel compito

Soluzione di gestione delle patch	CPO	CBO	CE	COSì	SOM	C
Esecuzione e della roadmap dei prodotti di gestione	A	C	R	C	C	I
Architettura e design per la gestione delle patch	A	I	R	C	I	
Sviluppo e configurazione della gestione delle patch	A		R	C		
Convalida e test della gestione delle patch	A	I	R	I	I	
NovitàAWS onboarding di account, applicazioni e server per l'applicazione di patch	A	C	R	I		

Soluzione di gestione delle patch	CPO	CBO	CE	COSÌ	SOM	C
Engagement e abilitazione degli utenti	A	R	I	I	I	
Feedback degli utenti e gestione dell'escalation	A	R		I	I	
Gestione delle modifiche di prodotto	A	R	C	I		
Gestione e risoluzione dei problemi	A		R	C		
Patching del server e conformità alle patch			C	C		AR
Configurazione della base di patch			C	R	A	C

Soluzione di gestione delle patch	CPO	CBO	CE	COSÌ	SOM	C
Reporting e conformità delle patch			C	R	AR	I

## Fasi successive

Questa guida ha descritto una soluzione di patch automatizzata per istanze mutabiliAWS e istanze on-premise in un ambiente cloud ibrido. Per creare la soluzione, si consiglia di consultare la documentazione per laAWS servizi descritti in questa guida. In caso di domande, contatta la tuaAWS account team per ricevere assistenza.

Per ulteriori informazioni, consulta la [.Altre risorse](#) sezione.

# Risorse aggiuntive

## AWSrisorse

- [AWSLinee guida prescrittive](#)
- [AWSdocumentazione](#)
- [AWSriferimenti generali](#)
- [AWSGlossario](#)

## AWSservizi

- [AWS CloudFormation](#)
- [Amazon CloudWatch](#)
- [Amazon EC2](#)
- [IAM](#)
- [AWS Lambda](#)
- [Amazon QuickSight](#)
- [AWS Systems Manager](#)

## Altre risorse

- [Come applicare patch alle istanze Amazon EC2 in sottoreti privateAWS Systems Manager](#)(AWSBlog di Management & Governance)
- [Come usa MoodyAWS Systems Managerper applicare patch server su più provider cloud](#)(AWSBlog di Management & Governance)
- [Configurazione diAWS Systems Managerper ambienti ibridi](#)(documentazione di Systems Manager)
- [Applicazione di patch multi-account e multi-regione centralizzata conAWS Systems ManagerAutomazione](#)(AWSBlog di Management & Governance)
- [Applicazione di patch delle istanze Amazon EC2 utilizzandoAWS Systems ManagerGestione Patch](#)(AWSBlog di Management & Governance)
- [Come applicare patch, ispezionare e proteggere i carichi di lavoro Microsoft Windows suAWS—Parte 1](#)(AWSBlog di sicurezza)

## Cronologia dei documenti

La tabella seguente descrive le modifiche importanti apportate a questa guida. Se desideri ricevere notifiche sugli aggiornamenti future, puoi sottoscrivere un [Avanzamento RSS](#).

Modifica	Descrizione	Data
<a href="#">Pubblicazione iniziale</a>	—	12 giugno 2020

# AWS Glossario delle linee guida prescrittive

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

## Numeri

### 7 R

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

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

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

## A

### ABAC

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

### servizi astratti

Vedi [servizi gestiti](#).

### ACIDO

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

### migrazione attiva-attiva

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

### migrazione attiva-passiva

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

### funzione aggregata

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

### Intelligenza artificiale

Vedi [intelligenza artificiale](#).

## AIOps

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

### anonimizzazione

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

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

### anti-modello

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

### controllo delle applicazioni

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

### portfolio di applicazioni

Una raccolta di informazioni dettagliate su ogni applicazione utilizzata da un'organizzazione, compresi i costi di creazione e manutenzione dell'applicazione e il relativo valore aziendale.

Queste informazioni sono fondamentali per [il processo di scoperta e analisi del portfolio](#) e aiutano a identificare e ad assegnare la priorità alle applicazioni da migrare, modernizzare e ottimizzare.

### intelligenza artificiale (IA)

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

### operazioni di intelligenza artificiale (AIOps)

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

## crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, consulta [ABAC 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 interrompere o causare danni a individui o organizzazioni.

### BCP

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

### grafico comportamentale

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

### sistema big-endian

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

### Classificazione binaria

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

### filtro Bloom

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

### distribuzioni blu/verdi

Una strategia di implementazione in cui si creano due ambienti separati ma identici. La versione corrente dell'applicazione viene eseguita in un ambiente (blu) e la nuova versione

dell'applicazione nell'altro ambiente (verde). Questa strategia consente di ripristinare rapidamente il sistema con un impatto minimo.

## bot

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

## botnet

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

## ramo

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

## accesso break-glass

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

## strategia brownfield

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

## cache del buffer

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

## capacità di business

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

## pianificazione della continuità operativa (BCP)

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

# C

## CAF

Vedi [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.

### crittografia lato client

Crittografia dei dati a livello locale, prima che il destinatario 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 sul blog](#) AWS Cloud Enterprise Strategy.

### cloud computing

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

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

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

## CMDB

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

### repository di codice

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

### cache fredda

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

### dati freddi

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

### visione artificiale (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, AWS Panorama offre dispositivi che aggiungono CV alle reti di telecamere locali e Amazon SageMaker fornisce algoritmi di elaborazione delle immagini per CV.

### deriva della configurazione

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

### database di gestione della configurazione (CMDB)

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



## Pacchetto di conformità

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

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

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

## CV

Vedi visione [artificiale](#).

## D

### dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

### classificazione dei dati

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

### deriva dei dati

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

## dati in transito

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

## rete di dati

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

## riduzione al minimo dei dati

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

## perimetro dei dati

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

## pre-elaborazione dei dati

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

## provenienza dei dati

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

## soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

## data warehouse

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

## linguaggio di definizione del database (DDL)

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

## linguaggio di manipolazione del database (DML)

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

## DDL

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

## deep ensemble

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

## deep learning

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

## defense-in-depth

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

## amministratore delegato

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

## implementazione

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

## Ambiente di sviluppo

[Vedi ambiente.](#)

### controllo di rilevamento

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

### mappatura del flusso di valore dello sviluppo (DVSM)

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

### gemello digitale

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

### tabella delle dimensioni

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

### disastro

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

### disaster recovery (DR)

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

## DML

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

### progettazione basata sul dominio

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

## DOTT.

Vedi [disaster recovery](#).

### rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, 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](#).

### edge computing

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

### crittografia

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

## chiave crittografica

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

## endianità

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

## endpoint

[Vedi](#) service endpoint.

## servizio endpoint

Un servizio che puoi ospitare in un cloud privato virtuale (VPC) da condividere con altri utenti. Puoi creare un servizio endpoint con AWS PrivateLink e concedere 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 pipeline CI/CD, l'ambiente di produzione è l'ultimo ambiente di implementazione.
- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

## epica

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

## ERP

Vedi [pianificazione delle risorse aziendali](#).

## analisi esplorativa dei dati (EDA)

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

## F

### tabella dei fatti

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

### fallire velocemente

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

## limite di isolamento dei guasti

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

## ramo di funzionalità

Vedi [filiale](#).

## caratteristiche

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

## importanza delle caratteristiche

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

## trasformazione delle funzionalità

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

## FGAC

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

## controllo granulare degli accessi (FGAC)

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

## migrazione flash-cut

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



## G

### blocco geografico

Vedi [restrizioni geografiche](#).

### limitazioni geografiche (blocco geografico)

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

### Flusso di lavoro di GitFlow

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

### strategia greenfield

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

### guardrail

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

## H

### AH

Vedi [disponibilità elevata](#).

## migrazione di database eterogenea

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

## alta disponibilità (HA)

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

## modernizzazione storica

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

## migrazione di database omogenea

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

## dati caldi

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

## hotfix

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

## periodo di hypercare

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

I

IaC

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

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi [Industrial Internet of Things](#).

infrastruttura immutabile

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

VPC in ingresso (ingress)

In un'architettura AWS multi-account, un VPC che accetta, ispeziona e indirizza le connessioni di rete dall'esterno di un'applicazione. 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.

I

## 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 la sezione [Interpretabilità dei modelli di machine learning con AWS](#).

## IoT

[Vedi Internet of Things.](#)

### libreria di informazioni IT (ITIL)

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

### gestione dei servizi IT (ITSM)

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

## ITIL

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

## ITSM

Vedi [Gestione dei servizi IT](#).

## L

### controllo degli accessi basato su etichette (LBAC)

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

### zona di destinazione

Una 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](#).

### migrazione su larga scala

Una migrazione di 300 o più server.

## BIANCO

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

### Privilegio minimo

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

### eseguire il rehosting (lift and shift)

Vedi [7 R](#).

### sistema little-endian

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

### ambienti inferiori

[Vedi ambiente](#).

## M

### machine learning (ML)

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

### ramo principale

Vedi [filiale](#).

### malware

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

## servizi gestiti

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

## sistema di esecuzione della produzione (MES)

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

## MAP

Vedi [Migration Acceleration Program](#).

## meccanismo

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

## account membro

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

## MEH

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

## Message Queuing Telemetry Transport (MQTT)

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

## microservizio

Un 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

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



## metadati di migrazione

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

## modello di migrazione

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

## Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione al Cloud. AWS MPA offre una valutazione dettagliata del portfolio (dimensionamento corretto dei server, prezzi, confronto del TCO, analisi dei costi di migrazione) e pianificazione della migrazione (analisi e raccolta dei dati delle applicazioni, raggruppamento delle applicazioni, prioritizzazione delle migrazioni e pianificazione delle ondate). [Lo strumento MPA](#) (richiede 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 nel 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, consulta la sezione [Valutazione della preparazione alla modernizzazione per le applicazioni nel cloud AWS](#).

## applicazioni monolitiche (monoliti)

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

## MAPPA

Vedi [Migration Portfolio Assessment](#).

## MQTT

Vedi [Message Queuing Telemetry Transport](#).

## classificazione multiclasse

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

## infrastruttura mutabile

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

## O

### OAC

Vedi [Origin Access Control](#).

### QUERCIA

Vedi [Origin Access Identity](#).

### OCM

Vedi [gestione delle modifiche organizzative](#).

### migrazione offline

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

### OI

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

### OLA

Vedi accordo a [livello operativo](#).

### migrazione online

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

### OPC-UA

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

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

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

## accordo a livello operativo (OLA)

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

## revisione della prontezza operativa (ORR)

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

## tecnologia operativa (OT)

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

## integrazione delle operazioni (OI)

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

## trail organizzativo

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

## gestione del cambiamento organizzativo (OCM)

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

## controllo dell'accesso all'origine (OAC)

In CloudFront, un'opzione avanzata per limitare l'accesso per proteggere i contenuti di Amazon Simple Storage Service (Amazon S3). OAC supporta tutti i bucket S3 in generale Regioni AWS, la

crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche e dirette al bucket S3.  
PUT DELETE

identità di accesso origine (OAI)

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

O

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. Per ulteriori informazioni, consulta la sezione [Abilitazione della persistenza dei dati nei microservizi](#).

## valutazione del portfolio

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

## predicate

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

## predicato pushdown

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

## controllo preventivo

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

## principale

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

## zone ospitate private

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

## controllo proattivo

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

## 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.

### 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.

### pubblica/iscriviti (pub/sub)

Un pattern 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).



## ransomware

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

## Matrice RASCI

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

## RCAC

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

## replica di lettura

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

## riprogettare

Vedi [7 Rs.](#)

## obiettivo del punto di ripristino (RPO)

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

## obiettivo del tempo di ripristino (RTO)

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

## rifattorizzare

Vedi [7 R.](#)

## Regione

Una raccolta di 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](#).

## rotazione

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

## controllo dell'accesso a righe e colonne (RCAC)

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

## RPO

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

## RTO

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

## runbook

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

# S

## SAML 2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità abilita il single sign-on (SSO) federato, in modo che gli utenti possano accedere AWS Management Console 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 AWS Secrets Manager, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, [consulta Secret](#) nella documentazione di Secrets Manager.

## controllo di sicurezza

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

## rafforzamento della sicurezza

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

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

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

## automazione della risposta alla sicurezza

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

## Crittografia lato server

Crittografia dei dati a destinazione, da parte 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](#).

## SIEM

Vedi il [sistema di gestione delle informazioni e degli eventi sulla sicurezza](#).

## punto di errore singolo (SPOF)

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

## SLAM

Vedi il contratto sul [livello di servizio](#).

## SLI

Vedi l'indicatore del [livello di servizio](#).

## LENTA

Vedi obiettivo del [livello di servizio](#).

## split-and-seed modello

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

## SPOF

Vedi [punto di errore singolo](#).

## schema a stella

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

## modello del fico strangolatore

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

## sottorete

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

## controllo di supervisione e acquisizione dati (SCADA)

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

## crittografia simmetrica

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

## test sintetici

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

# T

## tags

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

## variabile di destinazione

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

## elenco di attività

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

## Ambiente di test

[Vedi ambiente.](#)

## training

Fornire dati da cui trarre ispirazione dal modello di machine learning. I dati di training devono contenere la risposta corretta. L'algoritmo di apprendimento trova nei dati di addestramento i pattern che mappano gli attributi dei dati di input al target (la risposta che si desidera prevedere).

Produce un modello di ML che acquisisce questi modelli. Puoi quindi utilizzare il modello di ML per creare previsioni su nuovi dati di cui non si conosce il target.

## Transit Gateway

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

## flusso di lavoro basato su trunk

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

## Accesso attendibile

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

## regolazione

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

## team da due pizze

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

# U

## incertezza

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



è causata dal rumore e dalla casualità insiti nei dati. Per ulteriori informazioni, consulta la guida [Quantificazione dell'incertezza nei sistemi di deep learning](#).

## compiti indifferenziati

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

## ambienti superiori

[Vedi ambiente.](#)

# V

## vacuum

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

## controllo delle versioni

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

## Peering VPC

Una connessione tra due 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 query moderatamente lente.

## funzione finestra

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

## Carico di lavoro

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

## flusso di lavoro

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

## VERME

Vedi [scrivere una volta, leggere molti](#).

## WQF

Vedi [AWS Workload Qualification Framework](#).

## scrivi una volta, leggi molte (WORM)

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

## Z

exploit zero-day

[Un attacco, in genere malware, che sfrutta una vulnerabilità zero-day.](#)

vulnerabilità zero-day

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

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.