Gestione dell'identità e dell'accesso per Cloud on VMware AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: Gestione dell'identità e dell'accesso per Cloud on VMware AWS

Table of Contents

Introduzione 1
Destinatari principali 2
Obiettivi aziendali specifici 2
Panoramica sulla gestione dell'identità 3
Federazione delle identità e SSO 4
Best practice generali 5
VMware servizi di gestione delle identità 7
VMware Console di servizi cloud 7
Gestione delle identità e degli accessi 7
AWS raccomandazioni 8
VMware vCenter Server 9
Gestione delle identità e degli accessi 9
AWS raccomandazioni 10
VMware Servizi correlati 12
VMware Cloud attivo AWS 12
Gestione delle identità e degli accessi 13
AWS raccomandazioni 14
VMware NSX 14
Gestione delle identità e degli accessi 15
AWS raccomandazioni 16
VMware Aria Operations for Logs 17
Gestione delle identità e degli accessi 17
AWS raccomandazioni 18
VMware Aria Operations per reti 18
Gestione delle identità e degli accessi 19
AWS raccomandazioni 19
VMware Operazioni Aria 19
Gestione delle identità e degli accessi 20
AWS consigli 20
VMware Recupero informatico in tempo reale 21
Gestione delle identità e degli accessi 21
AWS raccomandazioni 22
VMware HCX 22
Gestione delle identità e degli accessi 23

AWS raccomandazioni ... 23
VMware Live Site Recovery ... 24
Gestione delle identità e degli accessi ... 24
AWS raccomandazioni ... 25
Gruppi e ruoli di esempio ... 26
Passaggi successivi ... 32
Risorse ... 33
AWS Risorse correlate ... 33
VMware documentazione ... 33
VMware Cloud attivo AWS ... 33
VMware vCenter Server e vCenter Single Sign-On ... 33
VMware NSX ... 34
VMware HCX ... 34
VMware Suite Aria e vRealize ... 34
VMware Ripristino del sito in tempo reale ... 34
VMware Recupero informatico in tempo reale ... 34
Cronologia dei documenti ... 35
Glossario ... 36
... 36
A ... 37
B ... 40
C ... 42
D ... 45
E ... 49
F ... 51
G ... 53
H ... 54
I ... 55
L ... 58
M ... 59
O ... 63
P ... 66
Q ... 69
R ... 69
S ... 72
T ... 76

U 77
V 78
W 78
Z 79
..... lxxxi

Gestione dell'identità e dell'accesso per VMware Cloud on AWS

Richard Milner-Watts, Abdenour Kansab e Chris Porter, Amazon Web Services

Vern Bolinius, VMware

settembre 2024 (storia del documento)

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on non AWS è più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

La gestione delle identità e degli accessi è il principio di limitare l'accesso ai sistemi solo agli utenti e alle applicazioni autorizzate, compresa la limitazione dell'accesso alle sole risorse di rete necessarie. Negli ambienti cloud, i controlli di gestione delle identità e degli accessi consistono in genere nelle policy e nei servizi utilizzati per identificare, autenticare e autorizzare utenti, gruppi di utenti e applicazioni.

VMware Cloud on AWS supporta i carichi di lavoro VMware basati su vSphere in. Cloud AWS Puoi utilizzare molti VMware servizi e strumenti per configurare, gestire, eseguire il backup, monitorare e analizzare questa infrastruttura cloud. Le funzionalità e i controlli utilizzati per gestire le identità e gli accessi variano a seconda dei servizi. Questo documento fornisce le migliori pratiche e consigli per la gestione dell'identità e dell'accesso ai seguenti VMware servizi:

- VMware Operazioni Aria
- VMware Operazioni Aria per i registri
- VMware Operazioni Aria per reti
- VMware Cloud attivo AWS
- VMware Console di servizi cloud
- VMware HCX
- VMware NSX
- VMware Ripristino informatico in tempo reale

- VMware Ripristino del sito in tempo reale
- VMware vCenter Server

Questa guida fornisce una panoramica e le migliori pratiche di gestione delle identità e degli accessi per VMware Cloud on AWS e VMware i servizi correlati. Include una breve descrizione di ogni servizio e illustra le considerazioni relative alla gestione di identità e accessi relativa a tale servizio. Forniamo anche consigli per configurare il servizio come parte di VMware Cloud on AWS.

> **Important**
>
> Molti dei VMware servizi discussi in questa guida vengono utilizzati in altre soluzioni cloud o locali VMware . I consigli e le best practice contenuti in questa guida sono specifici per VMware Cloud on AWS. pertanto potrebbero non essere applicabili ad altri ambienti.

Destinatari principali

Questa guida è destinata agli architetti e ai tecnici della sicurezza responsabili dell'implementazione di VMware Cloud on AWS nel loro ambiente cloud o ibrido.

Obiettivi aziendali specifici

Questa guida consente di eseguire le operazioni seguenti:

1. Comprendi i vari controlli di gestione delle identità e degli accessi per VMware Cloud on AWS e VMware i servizi correlati
2. Acquisisci familiarità con le migliori pratiche consigliate che ti aiutano a gestire in sicurezza VMware Cloud su AWS
3. Scoprire le opzioni disponibili per l'autenticazione federata tramite un provider di identità esterno

Panoramica sulla gestione dell'identità

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on non AWS è più rivenduto né dai suoi partner di canale. AWS Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware utilizza i seguenti concetti standard del settore e la gerarchia delle identità per gestire l'identificazione, l'autenticazione e l'autorizzazione:

- Gli utenti sono le persone che accedono all'ambiente con qualche ruolo. È possibile creare utenti locali oppure utilizzare la federazione per autenticare gli utenti da un gestore dell'identità digitale esterno. Per ulteriori informazioni, consulta Federazione delle identità e SSO.
- I gruppi costituiscono un meccanismo per raggruppare logicamente un insieme di utenti. Ciò consente di concedere autorizzazioni coerenti agli utenti riducendo il sovraccarico amministrativo. I ruoli vengono utilizzati per concedere autorizzazioni a un utente o a un gruppo. Per ulteriori informazioni, consulta Ruoli e autorizzazioni nell'SDDC (documentazione). VMware
- Organizations in VMware Cloud controllano l'accesso a uno o più VMware servizi. Gli utenti e i gruppi devono appartenere a un'organizzazione per poter accedere ai servizi dell'organizzazione. È possibile abilitare la funzionalità Identity Governance and Administration per consentire alle identità federate di richiedere in modalità self-service l'iscrizione a un'organizzazione. VMware Per ulteriori informazioni, consulta VMware Console di servizi cloud.

Le autorizzazioni possono concedere l'accesso a un oggetto specifico oppure possono essere ereditate dagli oggetti padre. Se a un utente o gruppo vengono assegnate più autorizzazioni sovrapposte, si applica l'autorizzazione più permissiva. Per ulteriori informazioni, vedere Ereditarietà gerarchica delle autorizzazioni (documentazione). VMware

È possibile utilizzare questi elementi strutturali per adottare una policy di privilegio minimo e stabilire limiti logici di accesso all'interno dell'infrastruttura in base ai requisiti degli utenti. Il privilegio minimo è il principio che consiste nel concedere agli utenti e alle applicazioni solo l'accesso minimo necessario per svolgere le loro attività. In caso di accesso non autorizzato, questa best practice può aiutare a limitare la capacità di un aggressore di causare danni o rubare dati sensibili. E anche per gli utenti autorizzati, questo principio può impedire agli utenti di accedere a dati a cui non dovrebbero avere

accesso. Consentire agli utenti di accedere solo alle risorse necessarie può anche migliorare la produttività, riducendo la necessità di chiedere assistenza per la risoluzione dei problemi.

Quando si utilizza VMware Cloud on AWS, esistono due servizi e strumenti principali per la gestione dell'identità e dell'accesso: e. VMware Console di servizi cloud VMware vCenter Server Più avanti in questa guida verranno presentati questi servizi in modo più dettagliato.

Federazione delle identità e SSO

Molte aziende vogliono creare una federazione con un gestore dell'identità digitale esterno. In questo modo puoi fornire un'esperienza di autenticazione unica (SSO) ai tuoi utenti. Sia VMware Cloud che vCenter Server supportano la federazione aziendale:

- VMware Cloud supporta il protocollo basato su Security Assertion Markup Language (SAML) 2.0 IdPs e supporta LDAP (Lightweight Directory Access Protocol). Per ulteriori informazioni, consulta Cos'è la federazione aziendale e come funziona con i servizi VMware cloud (documentazione). VMware
- Quando si utilizza vCenter Server on VMware Cloud on AWS, la federazione a vCenter Server utilizzando un IdP esterno non è attualmente supportata. È possibile usare solo l'IdP integrato, che supporta l'utilizzo di Microsoft Active Directory tramite LDAP. Per ulteriori informazioni, vedere Identity Sources for vCenter Server with vCenter Single Sign-On (documentazione). VMware

Alcuni degli altri VMware servizi correlati descritti in questa guida supportano anche la federazione diretta da un IdP. Tuttavia, la configurazione della federazione in ogni servizio crea ulteriori punti di gestione degli utenti e diventa difficile da gestire. Puoi invece utilizzare gruppi e ruoli nella VMware Cloud Services Console per utilizzare una fonte di identità comune e configurare le autorizzazioni per altri servizi VMware cloud. Inoltre, è possibile configurare la Hybrid Linked Mode per usare le stesse identità con un'istanza di vCenter Server on-premise. Ciò riduce il numero di punti di federazione e gestione delle identità a due servizi. Per ulteriori informazioni sulla modalità ibrida collegata, consulta Configurazione della modalità ibrida collegata (VMware documentazione).

Best practice generali

Comunicazione

A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

Important

Molti dei VMware servizi descritti in questa guida vengono utilizzati in altre VMware soluzioni cloud o locali. I consigli e le best practice contenuti in questa guida sono specifici per VMware Cloud on AWS. pertanto potrebbero non essere applicabili ad altri ambienti.

Prendi in considerazione i seguenti AWS consigli per gestire l'identità e l'accesso alla tua infrastruttura VMware cloud:

- Applica una policy di privilegio minimo. Usa il controllo degli accessi basato sui ruoli (RBAC) per concedere le autorizzazioni e gli accessi minimi necessari agli utenti per svolgere la loro funzione.
- Quando possibile, concedi le autorizzazioni ai gruppi invece che a singoli utenti.
- Evita di configurare utenti locali. Autentica gli utenti con un gestore dell'identità digitale federata esterno.
- Configura l'autenticazione a più fattori per tutti gli utenti.
- La tua policy in materia di password dovrebbe includere i requisiti di efficacia e rotazione della password.
- Documenta una procedura rivoluzionaria per assumere il pieno controllo amministrativo sull' VMwareorganizzazione e sui servizi correlati. Il termine "break glass", che prende il nome dall'azione di rompere il vetro per attivare un allarme antincendio, si riferisce a un mezzo che consenta a una persona di ottenere rapidamente l'accesso amministrativo in circostanze eccezionali, utilizzando un processo approvato e verificato.
- Se disponi di data center on-premise o di più istanze vCenter Server, usa la Hybrid Linked Mode per connettere l'istanza cloud di vCenter Server con il dominio vCenter Single Sign-On on-premise. Ciò consente di gestire le risorse cloud e on-premise da un'unica interfaccia vSphere Client.

- Quando possibile, configura gli endpoint di gestione, come vCenter Server, HCX Cloud Manager e NSX Manager, in modo che siano accessibili solo dalle reti interne, anziché dalla rete Internet pubblica.
- Non utilizzare credenziali locali, come l'account cloudadmin, per scopi amministrativi. Riserva questi account all'utilizzo nella procedura break-glass. Le azioni eseguite usando account utente amministrativi locali non possono essere attribuite a una persona specifica, quindi tali account possono essere utilizzati per apportare modifiche senza responsabilità.
- Modifica le password per gli account locali, come utenti root e amministrativi, inserendo valori efficaci e archivia queste credenziali in modo sicuro in un archivio di password verificato. Stabilisci un processo di approvazione per concedere l'accesso a queste password.
- Se le credenziali locali persistono per lunghi periodi, ad esempio per più mesi o più, stabilisci un processo per la rotazione delle credenziali (ad esempio, se utilizzi VMware HCX per estendere una rete).

Questi consigli si applicano a tutte le configurazioni del servizio per Cloud on VMware . VMware AWS Informazioni aggiuntive per ogni servizio sono riportate più avanti in questa guida.

VMware servizi di gestione delle identità

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

Quando si utilizza VMware Cloud on AWS, esistono due servizi e strumenti principali per la gestione dell'identità e dell'accesso: VMware Console di servizi cloud eVMware vCenter Server.

VMware Console di servizi cloud

VMware Cloud Services Console (VMware documentazione) ti aiuta a gestire il tuo portafoglio di servizi VMware Cloud, che include VMware Cloud on AWS. Con questo servizio è possibile:

- Gestire entità come utenti e gruppi
- Gestisci le organizzazioni, che controllano l'accesso ad altri servizi cloud, come VMware Live Cyber Recovery e VMware Aria Suite
- Assegnare ruoli a risorse e servizi
- Visualizza le OAuth applicazioni che hanno accesso alla tua organizzazione
- Configurare la federazione aziendale per l'organizzazione
- Abilita e distribuisci servizi VMware cloud, come VMware Aria e VMware Cloud on AWS
- Gestire la fatturazione e gli abbonamenti
- Richiedi assistenza VMware

Gestione delle identità e degli accessi

Configurando correttamente utenti, gruppi, ruoli e organizzazioni in VMware Cloud Services Console, puoi implementare una politica di accesso con privilegi minimi.

La protezione dell'accesso alla VMware Cloud Services Console è fondamentale perché gli utenti amministrativi di questo servizio possono modificare le autorizzazioni in tutto l'ambiente VMware

cloud e accedere a informazioni sensibili, come le informazioni di fatturazione. Per accedere a tutte le funzionalità della console, come la fatturazione e l'assistenza, gli utenti devono inoltre essere collegati a un profilo VMware Customer Connect (formalmente noto come My VMware).

In VMware Cloud Services Console, utilizzi i seguenti tipi di ruoli per concedere autorizzazioni a utenti e gruppi:

- Ruoli organizzativi: questi ruoli riguardano direttamente l'organizzazione VMware Cloud e concedono le autorizzazioni all'interno della VMware Cloud Services Console. Esistono due ruoli standard. Il ruolo del Proprietario dell'organizzazione dispone delle autorizzazioni complete per amministrare l'organizzazione. Il ruolo di membro dell'organizzazione ha accesso in lettura alla VMware Cloud Services Console. Per ulteriori informazioni, consulta Quali ruoli organizzativi sono disponibili nei servizi VMware cloud (VMwaredocumentazione).
- Ruoli di servizio – Questi ruoli consentono di assegnare le autorizzazioni per utilizzare un servizio specifico. Ad esempio, un'entità con il ruolo del servizio DR Admin può amministrare VMware Live Cyber Recovery nella console di servizio dedicata. Ogni servizio disponibile all'interno dell'organizzazione ha uno o più ruoli di servizio associati. Per ulteriori informazioni sui ruoli di servizio disponibili, consulta la VMware documentazione del servizio di interesse.

La VMware Cloud Services Console supporta le politiche di autenticazione. Queste possono stabilire che un utente debba fornire un secondo token di autenticazione al momento dell'accesso, noto anche come autenticazione a più fattori (MFA).

Per ulteriori informazioni sulla gestione dell'identità e dell'accesso in questo servizio, vedere Identity and Access Management (VMware documentazione).

AWS raccomandazioni

Oltre aBest practice generali, AWS consiglia quanto segue quando si configura VMware Cloud Services Console for VMware Cloud su AWS:

- Quando crei un'organizzazione, utilizza un profilo VMware Customer Connect e un indirizzo email aziendale associato che non appartenga a un individuo, come vmwarecloudroot@example.com. Questo account deve essere considerato come un account di servizio o root, ed è necessario controllarne l'utilizzo e limitare l'accesso all'account di posta elettronica. Configura immediatamente la federazione dell'account con il tuo gestore dell'identità digitale in modo che gli utenti possano accedere all'organizzazione senza utilizzare questo account. Riserva questo account all'uso in procedure break-glass per risolvere i problemi con il gestore dell'identità digitale federato.

- Utilizza identità federate per consentire all'organizzazione l'accesso ad altri servizi cloud, come VMware Live Cyber Recovery. Non gestite singolarmente gli utenti o la federazione in più servizi. Questo semplifica la gestione dell'accesso a più servizi, ad esempio nel caso di utenti che entrano in azienda o che la lasciano.
- Assegna il ruolo di Proprietario dell'organizzazione con parsimonia. Le entità con questo ruolo possono concedersi l'accesso completo a tutti gli aspetti dell'organizzazione e a tutti i servizi cloud associati.

VMware vCenter Server

VMware vCenter Server (VMwaresito Web) è un piano di gestione per l'amministrazione degli ambienti VMware vSphere. In vCenter Server, è possibile gestire le entità che possono accedere alle risorse vSphere, come le macchine virtuali, e accedere ai componenti aggiuntivi, come VMware HCX e Live Site Recovery. VMware Puoi gestire vCenter Server tramite l'applicazione vSphere Client. In vCenter Server è possibile:

- Gestione di macchine virtuali, VMware ESXi host e storage VMware vSAN
- Configurare e gestire vCenter Single Sign-On

Se disponi di data center locali, puoi utilizzare la Hybrid Linked Mode per collegare l'istanza cloud di vCenter Server a un dominio vCenter Single Sign-On on-premise. Se il dominio vCenter Single Sign-On contiene più istanze di vCenter Server connesse tramite Enhanced Linked Mode, tutte queste istanze sono collegate al tuo SDDC cloud. Utilizzando questa modalità, è possibile visualizzare e gestire i data center on-premise e cloud da un'unica interfaccia vSphere Client e migrare i carichi di lavoro tra il data center on-premise e il cloud SDDC. Per ulteriori informazioni, vedere Configurazione della modalità ibrida collegata (VMware documentazione).

Gestione delle identità e degli accessi

Nei software-defined data center (SDDCs) (VMware sito Web) per VMware Cloud on AWS, il modo in cui si utilizza vCenter Server è simile a un SDDC locale. La differenza principale è che VMware Cloud on è un servizio gestito. AWS Pertanto, VMware è responsabile di alcune attività amministrative, come la gestione di host, cluster e macchine virtuali di gestione. Per ulteriori informazioni, consulta Cosa c'è di diverso nel cloud? e Autorizzazioni globali (VMware documentazione).

Poiché VMware esegue alcune attività amministrative per l'SDDC, un amministratore cloud richiede meno privilegi rispetto a un amministratore di un data center locale. Quando crei un VMware Cloud

su AWS SDDC, viene creato automaticamente un utente cloudadmin a cui viene assegnato il ruolo (documentazione). CloudAdminVMware È possibile utilizzare questo account utente locale privilegiato per accedere a vCenter Server e vCenter Single Sign-On. Gli utenti che hanno il ruolo di servizio VMware Cloud on AWS Administrator o Administrator (Delete Restricted) nella VMware Cloud Services Console possono ottenere le credenziali per l'utente cloudadmin. Il CloudAdminruolo dispone delle autorizzazioni massime possibili in vCenter Server for VMware a Cloud AWS on SDDC. Per ulteriori informazioni su questo ruolo di servizio, vedere CloudAdmin Privileges (documentazione). VMware L'utente cloudadmin è l'unico utente locale disponibile per vCenter Server in Cloud on. VMware AWS Per concedere l'accesso ad altri utenti, utilizza un'origine di identità esterna.

vCenter Single Sign-On è un broker di autenticazione che fornisce un'infrastruttura di scambio di token di sicurezza. Quando un utente si autentica su vCenter Single Sign-On, riceve un token che può essere usato per l'autenticazione con vCenter Server e altri servizi aggiuntivi tramite chiamate API. L'utente cloudadmin può configurare un'origine di identità esterna per vCenter Server. Per ulteriori informazioni, vedere Identity Sources for vCenter Server with vCenter Single Sign-On (documentazione). VMware

In vCenter Server si utilizzano i seguenti tre tipi di ruoli per concedere autorizzazioni a utenti e gruppi:

- Ruoli di sistema – Non è possibile modificare o eliminare questi ruoli.
- Ruoli di esempio – Rappresentano combinazioni di attività eseguite di frequente. È possibile copiare, modificare o eliminare questi ruoli.
- Ruoli personalizzati – Se il sistema e i ruoli di esempio non forniscono il controllo degli accessi desiderato, è possibile creare ruoli personalizzati in vSphere Client. È possibile duplicare e modificare un ruolo esistente oppure crearne uno nuovo. Per ulteriori informazioni, vedere Create a vCenter Server Custom Role (VMware documentazione).

È possibile assegnare un solo ruolo a un utente o gruppo per ogni oggetto nell'inventario SDDC. Se, per un singolo oggetto, un utente o un gruppo richiede una combinazione di ruoli incorporati, sono disponibili due opzioni. La prima consiste nel creare un ruolo personalizzato con le autorizzazioni richieste. La seconda consiste nel creare due gruppi, assegnare un ruolo predefinito a ciascuno di essi e quindi aggiungere l'utente a entrambi i gruppi.

AWS raccomandazioni

Oltre aBest practice generali, AWS consiglia quanto segue quando si configura vCenter Server VMware for Cloud su: AWS

- Usa l'account utente cloudadmin per configurare un'origine di identità esterna in vCenter Single Sign-On. Assegna gli utenti appropriati dall'origine di identità esterna da utilizzare per scopi amministrativi, quindi interrompi l'utilizzo dell'utente cloudadmin. Per le best practice per la configurazione di vCenter Single Sign-On, vedere Information Security and Access for vCenter Server (documentazione). VMware
- In vSphere Client, aggiorna le credenziali dell'utente cloudadmin per ogni istanza di vCenter Server con un nuovo valore, quindi archiviale in modo sicuro. Questa modifica non si riflette nella Cloud Services Console. VMware Ad esempio, la visualizzazione delle credenziali tramite Cloud Services Console mostra il valore originale.

> **Note**
>
> Se le credenziali di questo account vengono perse, l' VMware assistenza può reimpostarle.

- Non utilizzare l'account cloudadmin per l'accesso. day-to-day Riserva questo account per l'uso come parte di una procedura Break-Glass.
- Limita l'accesso a vCenter Server alle sole reti private.

VMware Servizi correlati

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

Questo capitolo fornisce le migliori pratiche e consigli per la gestione dell'identità e dell'accesso per i seguenti VMware servizi relativi a VMware Cloud on AWS:

- Servizi gestiti tramite VMware Cloud Services Console:
  - VMware Cloud attivo AWS
  - VMware NSX
  - VMware Aria Operations for Logs
  - VMware Aria Operations per reti
  - VMware Operazioni Aria
  - VMware Recupero informatico in tempo reale
- Servizi gestiti tramite VMware vCenter Server:
  - VMware HCX
  - VMware Live Site Recovery

Questa guida fornisce una breve descrizione di ogni servizio, illustra i controlli di accesso e gestione delle identità per quel servizio e include AWS consigli per configurare tale servizio come parte di VMware Cloud on. AWS

VMware Cloud attivo AWS

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on non AWS è più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware Cloud on AWS (VMware documentazione) è un servizio progettato congiuntamente da AWS e per aiutarti VMware a migrare ed estendere gli ambienti locali basati su VMware vSphere a. Cloud AWS

Puoi accedere a VMware Cloud on AWS tramite VMware Cloud Services Console, se fai parte di un'organizzazione che concede l'accesso a questo servizio. In VMware Cloud on AWS, puoi:

- Creare ed eliminare SDDCs.
- Amministrare i gruppi SDDC.
- Amministrazione SDDCs, inclusi i parametri di rete e del cluster.
- Accedi alle credenziali utente cloudadmin per VMware vCenter Server. Per ulteriori informazioni su questo utente, consulta VMware vCenter Server in questa guida.
- Accedi alle credenziali utente cloud_admin per NSX. VMware Per ulteriori informazioni su questo utente, consulta VMware NSX in questa guida.
- Abilita e distribuisci servizi aggiuntivi all'interno SDDCs, come Live Site Recovery e HCX. VMware VMware
- Accedi alle console per servizi aggiuntivi, tra cui HCX e Live Site Recovery. VMware

Gestione delle identità e degli accessi

Utilizzi VMware Cloud Services Console per gestire le identità e l'accesso a Cloud on. VMware AWS Per VMware Cloud on AWS, sono disponibili i seguenti ruoli di servizio:

- Amministratore: questo ruolo ha pieno accesso a VMware Cloud on AWS.
- Amministratore (eliminazione limitata): questo ruolo ha pieno accesso a VMware Cloud on AWS, escluse le operazioni di eliminazione SDDC.
- NSX Cloud Admin
- NSX Cloud Auditor

> **Note**
>
> NSX Cloud Admin e NSX Cloud Auditor sono correlati all'uso di NSX. VMware Per ulteriori informazioni, consulta VMware NSX.

Uno dei due ruoli Administrator è necessario per accedere a un SDDC all'interno del portale di Cloud Services. Gli utenti privi di uno dei due ruoli NSX Cloud non possono accedere alla scheda Networking e sicurezza dell'SDDC all'interno del portale dei servizi cloud, e non possono accedere alle credenziali di amministratore di NSX.

AWS raccomandazioni

Oltre aBest practice generali, AWS consiglia quanto segue quando si configura VMware Cloud su AWS:

- Per concedere l'accesso agli amministratori, usa solo il ruolo Administrator (Delete Restricted). Riserva il ruolo Administrator per l'accesso break-glass quando è necessario eliminare un SDDC.
- Non concedere i ruoli NSX agli utenti che non hanno bisogno di accedere alle configurazioni di rete e firewall. Per ulteriori informazioni sul tagging, consulta VMware NSXin questa guida.
- Modifica le password dell'account utente locale cloudadmin inserendo valori efficaci e memorizza queste credenziali in modo sicuro in un archivio di password verificato. È possibile modificare questa password in VMware vCenter Server utilizzando vSphere Web Client.

VMware NSX

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware NSX (VMwaredocumentazione) fornisce un livello di virtualizzazione della rete che riproduce il modello Open Systems Interconnection (OSI) dal livello 2 al livello 7, con funzionalità tra cui switching, routing e firewall. Esistono due versioni di NSX. La versione originale (NSX-V) richiede anche l'implementazione di vCenter Server. La versione più recente (NSX-T) è disaccoppiata da vCenter Server, che consente il supporto per architetture ibride. VMware Cloud AWS on utilizza NSX-T.

NSX, insieme a vSphere e vSAN, è un componente fondamentale di Cloud on. VMware AWS NSX fornisce tutte le funzionalità di rete all'interno di un SDDC e gestisce l'interazione tra la rete overlay

e i componenti AWS nativi che costituiscono l'underlay di rete. NSX è strettamente associato ad altri servizi, come vCenter Server e VMware HCX, che utilizzano NSX per gestire le risorse. APIs

In NSX, è possibile:

- Gestire lo switching e il routing
- Gestisci i firewall, incluso l'utilizzo di un firewall distribuito per l'ispezione in linea tra o tra la rete e la rete Internet pubblica VMs
- Gestisci reti private virtuali () VPNs
- Configurare il Protocollo di configurazione per host dinamico (DHCP) e il sistema dei nomi di dominio (DNS)

Puoi accedere a NSX dalla console dei servizi VMware cloud o tramite l'interfaccia utente web (UI) dedicata di NSX Manager. L'interfaccia utente web di NSX Manager offre alcune funzionalità aggiuntive che non sono disponibili nella VMware Cloud Services Console. Per ulteriori informazioni, consulta SDDC Network Administration with NSX Manager (documentazione)VMware .

Tieni presente quanto segue quando accedi a NSX in VMware Cloud su: AWS

- Per accedere a NSX tramite la VMware Cloud Services Console, devi avere il ruolo VMware Cloud on AWS Administrator. Puoi accedere a NSX nella scheda Rete e sicurezza dell'SDDC. Per ulteriori informazioni su questo ruolo, consulta l'argomento VMware Cloud attivo AWS in questa guida.
- Puoi aprire l'interfaccia utente web di NSX Manager selezionando il collegamento nella scheda Impostazioni dell'SDDC o selezionando Apri NSX Manager nella pagina di riepilogo dell'SDDC. Per ulteriori informazioni, consulta Open NSX Manager (VMware documentazione).
- Se l'SDDC è in modalità Payment Card Industry Data Security Standard (PCI DSS), non è possibile accedere a NSX tramite la scheda Networking and Security nella Cloud Services Console. VMware ma devi usare l'interfaccia utente web di NSX Manager.

Gestione delle identità e degli accessi

Utilizzi VMware Cloud Services Console per gestire le identità e l'accesso a NSX. VMware Per NSX in VMware Cloud on AWS, sono disponibili i seguenti ruoli di servizio:

- NSX Cloud Admin: questo ruolo può amministrare le funzionalità VMware NSX con Cloud on. VMware AWS

- NSX Cloud Auditor – Questo ruolo può visualizzare le impostazioni e gli eventi del servizio NSX ma non può apportare modifiche.

> **Note**
>
> Nonostante i loro nomi, questi ruoli non sono correlati al servizio VMware NSX Cloud.

I seguenti utenti possono accedere a NSX:

- L'utente locale cloud_admin, che è un utente NSX locale integrato e altamente privilegiato. Gli utenti che hanno il ruolo NSX Cloud Admin possono accedere alle credenziali di questo account utente. Nonostante i nomi simili, l'utente cloud_admin è diverso dall'utente locale di vCenter Single Sign-On cloudadmin@vmc.local.
- Utenti a cui è stato assegnato il ruolo di servizio NSX Cloud Admin o il ruolo di servizio NSX Cloud Auditor nella VMware Cloud Services Console. Questi utenti potrebbero essere utenti della VMware Cloud Services Console o utenti federati esternamente.
- Utenti a cui è stato concesso l'accesso diretto a NSX da un'origine di identità tramite LDAP.

AWS raccomandazioni

Oltre aBest practice generali, AWS consiglia quanto segue per la configurazione di NSX for VMware Cloud su: AWS

- Se la tua azienda ha utenti responsabili della gestione della rete e dei firewall ma non della gestione SDDCs, concedi a questi utenti uno dei ruoli NSX, ma non il ruolo di amministratore. Questi utenti devono accedere a NSX tramite l'interfaccia utente web di NSX Manager.
- Modifica le password dell'account utente locale cloud_admin inserendo valori efficaci e memorizza queste credenziali in modo sicuro in un archivio di password verificato. Per modificare questa password, è necessario contattare VMware l'assistenza.
- Non concedere l'accesso a utenti esterni direttamente all'interno di NSX. Configura invece la federazione aziendale nella VMware Cloud Services Console, quindi utilizza ruoli e gruppi per concedere l'accesso a questo servizio.

VMware Aria Operations for Logs

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware Aria Operations for Logs (VMware documentazione), precedentemente VMwarevRealize Log Insight Cloud, è uno strumento di archiviazione e analisi dei log che consente di visualizzare e interrogare i dati di registro prodotti dal sistema. VMware SDDCs In VMware Aria Operations for Logs, puoi:

- Integrare istanze on-premise di vRealize Operations
- Raccogli e analizza tutti i tipi di dati di log generati dalla macchina
- Configurazione degli avvisi
- Monitora e analizza i log di altri servizi VMware

Esistono due versioni di questo servizio centralizzato di gestione dei registri. VMware vRealize Log Insight è una versione locale che può essere eseguita come appliance all'interno dell'SDDC. VMware Aria Operations for Logs è una versione software-as-a-service (SaaS). VMware Cloud on AWS utilizza la versione cloud come servizio di registrazione predefinito e questo non può essere modificato. Se utilizzi la versione on-premise, devi inoltrare i log dall'istanza cloud all'istanza on-premise.

VMware Aria Operations for Logs è inclusa in VMware Cloud on. AWS La versione inclusa ha una capacità di ingestione e un periodo di conservazione dell'archiviazione limitati. Se necessario, puoi passare a un abbonamento premium per aumentare questi limiti. Per ulteriori informazioni, consulta Abbonamenti e fatturazione (documentazione)VMware .

Gestione delle identità e degli accessi

Utilizzi VMware Cloud Services Console per gestire le identità e l'accesso ad VMware Aria Operations for Logs. VMware Aria Operations for Logs utilizza gli stessi utenti, comprese le identità federate, e gli stessi gruppi che hai configurato in Cloud Services Console. VMware Per concedere le autorizzazioni per questo servizio, puoi assegnare un ruolo di servizio o configurare un ruolo

personalizzato all'interno VMware di Aria Operations for Logs. Per ulteriori informazioni, consultate Service Roles (documentazione)VMware .

VMware vRealize Log Insight ha due ruoli predefiniti. Il ruolo Administrator ha accesso e controllo completi, mentre il ruolo User ha accesso in lettura e può creare pannelli di controllo. È possibile utilizzare ruoli personalizzati per concedere l'accesso solo a set di dati specifici. Questi set di dati contengono filtri che limitano i dati di log disponibili per l'utente. Per ulteriori informazioni, vedere Creare un set di dati (VMware documentazione).

AWS raccomandazioni

Segui le Best practice generali descritte in precedenza in questa guida. Non abbiamo consigli aggiuntivi per la gestione delle identità e degli accessi in questo servizio.

VMware Aria Operations per reti

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware Aria Operations for Networks, precedentemente VMware vRealize Network Insight Cloud, è una versione SaaS di vRealize Network Insight. VMware vRealize Network Insight (VMware documentazione) ti aiuta a comprendere i flussi di traffico per i tuoi carichi di lavoro. È possibile usare questo servizio per diagnosticare problemi di rete e modellare le regole del firewall per supportare la segmentazione dei carichi di lavoro. In VMware Aria Operations for Networks, puoi:

- Visualizzare i propri ambienti ibridi e multi-cloud
- Risolvere i problemi e analizzare i flussi di traffico
- Individuare e analizzare le applicazioni
- Mappare le dipendenze tra i carichi di lavoro

Esistono tre versioni di questo servizio. VMware vRealize Network Insight è una on-premises-only versione. VMware Aria Operations for Networks è una versione SaaS. vRealize Network Insight

Universal può essere distribuito come soluzione locale o come soluzione SaaS cloud federata. Tutte le versioni sono compatibili con Cloud on. VMware AWS

Gestione delle identità e degli accessi

Utilizzi VMware Cloud Services Console per gestire le identità e l'accesso ad VMware Aria Operations for Networks. VMware Aria Operations for Networks utilizza gli stessi utenti, incluse le identità federate, e gli stessi gruppi che hai configurato in VMware Cloud Services Console. Per VMware Aria Operations for Networks, sono disponibili i seguenti ruoli di servizio:

- Amministratore – Questo ruolo ha accesso e controllo completi.
- Membro – Questo ruolo ha un accesso limitato.
- revisore contabile – Questo ruolo ha accesso di sola lettura.

AWS raccomandazioni

Segui le Best practice generali descritte in precedenza in questa guida. Non abbiamo consigli aggiuntivi per la gestione delle identità e degli accessi in questo servizio.

VMware Operazioni Aria

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on non AWS è più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware Aria Operations (VMware documentazione), precedentemente VMware vRealize Operations Cloud, è una piattaforma di gestione delle operazioni per VMware Cloud on. AWS Questo servizio utilizza l'intelligenza artificiale e il machine learning (AI/ML) per aiutarti a ottimizzare, pianificare e scalare le applicazioni e l'infrastruttura nelle tue implementazioni del cloud ibrido. In VMware Aria Operations, puoi:

- Visualizzare consigli di ottimizzazione basati su AI/ML per prestazioni e capacità
- La gestione delle configurazioni delle risorse e della conformità

- Accedere agli strumenti per la risoluzione dei problemi, ad esempio per l'assistenza dei clienti o per rispondere agli avvisi
- Utilizza i management pack (VMware documentazione) per espandere le funzionalità di monitoraggio, risoluzione dei problemi e riparazione di questo servizio

Esistono due versioni di questo servizio di gestione delle operazioni. VMware vRealize Operations è una versione locale che può essere eseguita come appliance all'interno dell'SDDC. VMware Aria Operations è una versione software-as-a-service (SaaS) di vRealize Operations. Entrambe le versioni sono compatibili con VMware Cloud on. AWS Poiché VMware Cloud on AWS è un servizio gestito e l'accesso ad alcune risorse è limitato, non tutte le funzionalità di vRealize Operations sono supportate. Per ulteriori informazioni, vedere Limitazioni note (VMware documentazione).

Gestione delle identità e degli accessi

Utilizzi VMware Cloud Services Console per gestire le identità e l'accesso ad VMware Aria Operations. VMware Aria Operations utilizza gli stessi utenti, incluse le identità federate, configurati in VMware Cloud Services Console. Per concedere le autorizzazioni per questo servizio, puoi assegnare un ruolo di servizio o configurare un ruolo personalizzato all'interno di Aria Operations. VMware Per ulteriori informazioni sui ruoli di servizio disponibili, consulta Ruoli e privilegi (VMware documentazione).

Sono disponibili tre ruoli predefiniti: amministratore GeneralUsere ReadOnly, se necessario, è possibile creare ruoli personalizzati per soddisfare requisiti di autorizzazioni specifici. È possibile creare gruppi per ridurre al minimo i sovraccarichi amministrativi causati dalla gestione delle autorizzazioni per più utenti.

La versione locale di VMware vRealize Operations supporta gli utenti locali e sia la versione cloud che quella locale supportano gli utenti federati. Tuttavia, la federazione degli utenti a un gestore dell'identità digitale esterno varia tra la versione on-premise e quella cloud di vRealize Operations. Per la versione on-premise, è possibile federare direttamente gli utenti di un IdP esterno tramite LDAP, oppure è possibile utilizzare le identità federate in vCenter Server. Per la versione cloud, si utilizzano gli stessi utenti, inclusi gli utenti federati, configurati in Cloud Services Console. VMware

AWS consigli

Oltre aBest practice generali, AWS consiglia quanto segue quando si configura VMware Aria Operations for VMware Cloud su AWS:

- Evita di federare direttamente gli utenti. Per la versione cloud, federate gli utenti nella VMware Cloud Services Console, quindi utilizzate ruoli e gruppi per concedere l'accesso a questo servizio. Per la versione on-premise del servizio, usa identità da un'origine autenticata o abilita l'autenticazione unica (SSO). Per ulteriori informazioni, consulta Fonti di autenticazione e Configurazione di una fonte Single Sign-On (documentazione)VMware .

VMware Recupero informatico in tempo reale

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware Live Cyber Recovery (VMware documentazione) è una soluzione di disaster recovery as a service (DRaaS) che offre un approccio a più livelli al disaster recovery. È possibile modificare i costi e i tempi per l'obiettivo del punto di ripristino (RPO) e l'obiettivo del tempo di ripristino (RTO) per soddisfare i requisiti per un determinato carico di lavoro. Questo aiuta a trovare un equilibrio tra una protezione affidabile e l'uso efficiente delle risorse di ripristino di emergenza. In VMware Live Cyber Recovery, puoi:

- Creare backup di macchine virtuali
- Archiviare i backup in un cloud storage durevole
- Scegliere tra opzioni di implementazione flessibili per gli obiettivi di ripristino, da quelle on-demand a quelle in modalità standby a caldo
- Configurazione personalizzata RPOs e RTOs

Gestione delle identità e degli accessi

Utilizzi VMware Cloud Services Console per gestire le identità e l'accesso a VMware Live Cyber Recovery. VMware Live Cyber Recovery utilizza gli stessi utenti, incluse le identità federate, e gli stessi gruppi che hai configurato in Cloud Services Console. VMware Per concedere le autorizzazioni per questo servizio, puoi assegnare un ruolo del servizio VMware Live Cyber Recovery o creare un ruolo personalizzato all'interno di Live Cyber Recovery. VMware Per ulteriori informazioni sui ruoli di

servizio disponibili, vedere Ruoli degli utenti finali di VMware Live Cyber Recovery (documentazione). VMware

VMware Live Cyber Recovery include diversi ruoli integrati che è possibile utilizzare per gestire il servizio:

- Administrator – Controllo completo, escluso l'accesso ai token API.
- Auditor – Accesso in sola lettura all'interfaccia utente, esclusa la gestione degli utenti. Accesso ai report di conformità.
- DR Admin – Crea, testa ed esegui piani di ripristino di emergenza.
- Backup Admin – Gestisci siti protetti e gruppi di protezione. Accesso al ripristino VMs.
- Plan Tester – Crea piani di ripristino di emergenza, esegui ripristini di prova.
- Amministratore SDDC: gestione SDDCs.

AWS raccomandazioni

Segui le Best practice generali descritte in precedenza in questa guida. Non abbiamo consigli aggiuntivi per la gestione delle identità e degli accessi in questo servizio.

VMware HCX

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware HCX (VMwaredocumentazione) è una piattaforma di mobilità delle applicazioni che consente la migrazione dei carichi di lavoro tra. SDDCs VMware HCX è incluso in VMware Cloud on AWS e può essere utilizzato per migrare i carichi di lavoro. In VMware HCX, puoi:

- Configurare mesh multisito tra SDDCs
- Estendere le reti tra i siti HCX
- Migrare le macchine virtuali

Gestione delle identità e degli accessi

Si utilizza VMware vCenter Server per gestire le identità e l'accesso a HCX. VMware VMware HCX richiede l'accesso ad altri VMware servizi per creare e gestire risorse e migrazioni, incluso l'accesso a vCenter Server e NSX. VMware HCX ha due servizi componenti:

- HCX Cloud Manager: nella console dei servizi VMware cloud, abiliti VMware HCX per l'SDDC. Questo installa l'appliance HCX Cloud Manager all'interno dell'SDDC selezionato. Per ulteriori informazioni, vedere Deploying the HCX Installer OVA nel vSphere Client (documentazione). VMware Dopo l'implementazione, è possibile utilizzare le credenziali cloudadmin di vCenter Server per accedere al servizio HCX Cloud Manager.
- HCX Connector – È possibile ottenere il file HCX Connector Open Virtualization Archive (OVA) tramite il servizio HCX Cloud Manager. Questo file viene utilizzato per installare un'appliance HCX Cloud Manager su qualsiasi istanza di vCenter Server, che configura tale istanza come origine di migrazione in HCX. VMware Ogni istanza di HCX Connector ha le proprie credenziali di amministratore e root.

Dopo aver distribuito entrambi i servizi componenti, è possibile accedere a VMware HCX tramite vCenter Server. Il gruppo Administrators di vCenter Single Sign-On riceve automaticamente il ruolo HCX Administrator. L'installazione di HCX introduce molti ruoli e privilegi aggiuntivi a vCenter Single Sign-On. Utilizzali per creare controlli di accesso dettagliati per VMware HCX, in base ai diversi tipi di utenti.

AWS raccomandazioni

Oltre aBest practice generali, AWS consiglia quanto segue quando si configura VMware HCX for VMware Cloud su: AWS

- Usa le regole del Gateway Firewall per limitare l'accesso alla rete al servizio HCX Cloud Manager.
- Memorizzate in modo sicuro le credenziali dell'amministratore e dell'utente root di HCX Connector on-premise. Valuta la possibilità di ruotare queste credenziali in base alle politiche aziendali. VMware gestisce queste credenziali per tuo conto per HCX Cloud Manager.
- Per un'istanza HCX Connector on-premise, valuta la possibilità di creare ruoli HCX personalizzati che soddisfino le esigenze dei diversi tipi di utenti HCX. Ad esempio, crea un ruolo più permissivo per gli utenti che configurano e amministrano HCX e crea un ruolo meno permissivo per gli utenti che gestiscono solo le migrazioni.

- Quando si associa VMware HCX a VMware Cloud on AWS, è necessario utilizzare l'utente cloudadmin.
- Quando si associa HCX Cloud a Cloud on AWS, l'autenticazione non è supportata tra VMware Cloud on SDDC e Active Directory. VMware AWS Per ulteriori informazioni, consulta [VMC on AWS] AD non supportato per la configurazione di HCX Cloud to Cloud (articolo 90433 della VMware Knowledge Base).

VMware Live Site Recovery

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

VMware Live Site Recovery (VMware documentazione) è una soluzione di disaster recovery as a service (DRaaS) su richiesta basata sul servizio VMware Site Recovery Manager per ambienti locali. In VMware Live Site Recovery, puoi:

- Implementa la replica, l'orchestrazione e l'automazione per proteggere i carichi di lavoro in caso di guasto del sito
- Crea una soluzione di end-to-end disaster recovery per contribuire a proteggere SDDCs

Gestione delle identità e degli accessi

Si utilizza VMware vCenter Server per gestire le identità e l'accesso a VMware Live Site Recovery. VMware Live Site Recovery esegue operazioni per conto degli utenti, come la replica o lo spegnimento di una macchina virtuale. VMware Live Site Recovery utilizza ruoli e privilegi per garantire che solo gli utenti con le autorizzazioni corrette possano eseguire operazioni di ripristino, come l'esecuzione di tutti i passaggi di un piano di ripristino.

Per ulteriori informazioni, vedere Privilegi, ruoli e autorizzazioni di VMware Live Site Recovery (documentazione). VMware

Se usi identità federate per accedere a vCenter Server, devi usare la Hybrid Linked Mode per aggiungere entità a questi gruppi. Per ulteriori informazioni, vedere Configurazione della modalità ibrida collegata (documentazione)VMware .

AWS raccomandazioni

Oltre aBest practice generali, AWS consiglia quanto segue per la configurazione di VMware Live Site Recovery for VMware Cloud su AWS:

- Assicurati che agli utenti siano assegnati gli stessi ruoli sia sul sito di origine che su quello di destinazione. Ciò garantisce che gli oggetti protetti e recuperati abbiano le stesse autorizzazioni.
- Utilizza la modalità Hybrid Linked per gestire le assegnazioni di ruoli per le identità federate all'interno di vCenter Server.
- VMware Live Site Recovery utilizza indirizzi IP privati solo all'interno dell'SDDC. Di conseguenzaBest practice generali, assicurati che il tuo VMware Cloud on AWS vCenter si risolva in un indirizzo IP privato.

Gruppi e ruoli di esempio

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on non AWS è più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

La tabella seguente fornisce un esempio di strategia di gestione delle identità e degli accessi per l'utilizzo di VMware Cloud on AWS. Descrive la persona dell'utente, i VMware servizi a cui la persona deve accedere, l'organizzazione e l'appartenenza al gruppo, i ruoli assegnati e il tipo di identità utilizzata (come utenti locali o identità federate). Utilizzando questa tabella come punto di partenza, è possibile progettare una strategia aziendale in grado di aderire alle best practice consigliate in questa guida.

Tipo di utente	Servizi a cui accede	VMware Nome del gruppo di esempio nel cloud	VMware Ruoli dei servizi cloud	Nome del gruppo di esempio di vCenter Single Sign-On	Ruolo di vCenter Single Sign-On	Origine dell'identità
Account break glass dell'organizzazione	VMware Console di servizi cloud	Nessuno	Titolare dell'organizzazione	Nessuno	Nessuno	Utente locale (indirizzo e-mail dell'account di servizio)
VMware amministratore	VMware Console di servizi cloud	`vmware_admins`	Titolare dell'organizzazione	`vmware_admins`	Amministratore	Provider di identità federate

Tipo di utente	Servizi a cui accede	VMware Nome del gruppo di esempio nel cloud	VMware Ruoli dei servizi cloud	Nome del gruppo di esempio di vCenter Single Sign-On	Ruolo di vCenter Single Sign-On	Origine dell'identità
	vCenter Server HCX VMware Ripristino del sito in tempo reale VMware Ripristino informatico in tempo reale vRealize Operations					
Amministratore di backup	vCenter Server	Nessuno	Nessuno	`vmware_backups`	Utente avanzato	Provider di identità federate

Tipo di utente	Servizi a cui accede	VMware Nome del gruppo di esempio nel cloud	VMware Ruoli dei servizi cloud	Nome del gruppo di esempio di vCenter Single Sign-On	Ruolo di vCenter Single Sign-On	Origine dell'identità
Amministratore del ripristino di emergenza	vCenter Server VMware Console di servizi cloud VMware Ripristino del sito in tempo reale VMware Ripristino informatico in tempo reale	`vmware_dr`	Membro dell'organizzazione Amministratore DR Amministratore DR SDDC	`vmware_dr`	SrmAdministrator HmsCloudAdmin	Provider di identità federate

Tipo di utente	Servizi a cui accede	VMware Nome del gruppo di esempio nel cloud	VMware Ruoli dei servizi cloud	Nome del gruppo di esempio di vCenter Single Sign-On	Ruolo di vCenter Single Sign-On	Origine dell'identità
VMware operatore	VMware Console di servizi cloud vCenter Server HCX vRealize Operations	`vmware_ops`	Membro dell'organizzazione v ROps Amministratore	`vmware_ops`	Utente avanzato	Provider di identità federate
Team di rete	VMware Console di servizi cloud vCenter Server	`vmware_networks`	Membro dell'organizzazione NSX Cloud Admin	`vmware_networks`	Readonly	Provider di identità federate

Tipo di utente	Servizi a cui accede	VMware Nome del gruppo di esempio nel cloud	VMware Ruoli dei servizi cloud	Nome del gruppo di esempio di vCenter Single Sign-On	Ruolo di vCenter Single Sign-On	Origine dell'identità
Team di sicurezza	VMware Console di servizi cloud vCenter Server HCX (accesso temporaneo) VMware Ripristino del sito in tempo reale VMware Ripristino informatico in tempo reale vRealize Operations	`vmware_security`	Membro dell'organizzazione v ROps ReadOnly	`vmware_security`	Readonly	Provider di identità federate

Tipo di utente	Servizi a cui accede	VMware Nome del gruppo di esempio nel cloud	VMware Ruoli dei servizi cloud	Nome del gruppo di esempio di vCenter Single Sign-On	Ruolo di vCenter Single Sign-On	Origine dell'identità
Revisori	VMware Console di servizi cloud vCenter Server	`vmware_audit`	Membro dell'organizzazione	`vmware_audit`	Readonly	Provider di identità federate

Passaggi successivi

Comunicazione

A partire dal 30 aprile 2024, VMware Cloud on AWS non sarà più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

Questa guida illustra le migliori pratiche consigliate per la gestione dell'identità e dell'accesso a VMware Cloud on AWS e ai VMware servizi correlati. Questi consigli hanno lo scopo di aiutarti a proteggere la tua infrastruttura cloud e cloud ibrido e prevenire accessi non autorizzati, ma sono anche pensati per essere scalabili ed efficienti. Assegnando prima gli utenti e poi i ruoli ai gruppi, è possibile concedere o limitare più rapidamente le autorizzazioni e ridurre al minimo il sovraccarico associato alla configurazione degli utenti individuali. Inoltre, usando la federazione con un gestore dell'identità digitale esterno e vCenter Single Sign-On, puoi fornire agli utenti un'esperienza Single Sign-On ottimale.

Usa la tabella Gruppi e ruoli di esempio per iniziare a progettare una strategia di gestione delle identità e degli accessi adatta alla tua azienda. Dopo aver letto i consigli contenuti in questa guida, ti suggeriamo di consultare i link forniti nella sezione Risorse. Queste risorse ti aiuteranno a saperne di più sui servizi VMware Cloud e su come configurare le migliori pratiche descritte in questa guida.

Risorse

> **Comunicazione**
>
> A partire dal 30 aprile 2024, VMware Cloud on non AWS è più rivenduto AWS né dai suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

AWS Risorse correlate

- VMware AWS Panoramica e modello operativo di Cloud on
- Opzioni di disaster recovery per carichi di lavoro su VMware Cloud on AWS
- Configurazione delle opzioni di storage offload per Cloud on VMware AWS
- Implementa un VMware SDDC utilizzando Cloud on AWS VMware AWS
- Esegui la migrazione da VMware SDDC a VMware Cloud utilizzando HCX AWS VMware

VMware documentazione

VMware Cloud attivo AWS

- Configurazione della federazione aziendale per i servizi cloud
- VMware Identity and Access Management per i servizi cloud

VMware vCenter Server e vCenter Single Sign-On

- Informazioni sulle autorizzazioni in vSphere
- Amministrazione di vSphere nel VMware cloud su AWS
- Autenticazione vSphere con vCenter Single Sign-On
- Configurazione delle origini di identità vCenter Single Sign-On
- Ereditarietà gerarchica delle autorizzazioni
- Sicurezza e accesso alle informazioni per vCenter Server
- Privilegi richiesti da vSphere per attività comuni

VMware NSX

- Guida all'amministrazione di NSX
- Sicurezza e accesso alle informazioni per il data center NSX-T

VMware HCX

- VMware Documentazione HCX
- VMware Requisiti relativi all'account utente e al ruolo di HCX

VMware Suite Aria e vRealize

- VMware Documentazione sulle operazioni di vRealize
- Ruoli e privilegi in vRealize Operations Cloud
- VMware Scheda tecnica di vRealize Log Insight
- Guida introduttiva a VMware Aria Operations for Logs
- VMware Documentazione sui servizi cloud
- Gestione degli utenti di vRealize Network Insight

VMware Ripristino del sito in tempo reale

- VMware Documentazione Live Site Recovery
- VMware Privilegi, ruoli e autorizzazioni di Live Site Recovery

VMware Recupero informatico in tempo reale

- VMware Documentazione Live Cyber Recovery
- VMware Ruoli degli utenti finali di Live Cyber Recovery

Cronologia dei documenti

Comunicazione

A partire dal 30 aprile 2024, VMware Cloud on non AWS è più rivenduto né dai AWS suoi partner di canale. Il servizio continuerà a essere disponibile tramite Broadcom. Ti invitiamo a contattare il tuo AWS rappresentante per i dettagli.

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

Modifica	Descrizione	Data
VMware offerte di servizi	Abbiamo sostituito VMware Cloud Disaster Recovery con VMware Live Cyber Recovery e Site Recovery con VMware Live VMware Site Recovery. Per ulteriori informazioni, consulta le note di rilascio di VMware Live Recovery.	4 settembre 2024
VMware Accesso HCX	Abbiamo aggiornato i AWS consigli per configurare VMware HCX for Cloud su. VMware AWS	5 giugno 2023
Pubblicazione iniziale	—	3 novembre 2022

AWS Glossario delle linee guida prescrittive

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

Numeri

7 R

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

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

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

Un metodo di migrazione 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 AIOps viene utilizzato nella strategia di AWS migrazione, consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

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

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

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, distribuisci la nuova versione e sostituisci la versione corrente nella sua interezza.

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

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

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

Un approccio alla sicurezza delle informazioni in cui una serie di meccanismi e controlli di sicurezza sono accuratamente stratificati su una rete di computer per proteggere la riservatezza,

l'integrità e la disponibilità della rete e dei dati al suo interno. Quando si adotta questa strategia AWS, si aggiungono più controlli a diversi livelli della AWS Organizations struttura per proteggere le risorse. Ad esempio, un defense-in-depth approccio potrebbe combinare l'autenticazione a più fattori, la segmentazione della rete e la crittografia.

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

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

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. 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 epopee della sicurezza AWS CAF includono la gestione delle identità e degli accessi, i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS , consulta la guida all'implementazione del programma.

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi il modello di base.

modello di fondazione (FM)

Una grande rete neurale di deep learning che si è addestrata su enormi set di dati generalizzati e non etichettati. FMs sono in grado di svolgere un'ampia varietà di attività generali, come

comprendere il linguaggio, generare testo e immagini e conversare in linguaggio naturale. Per ulteriori informazioni, consulta Cosa sono i modelli Foundation.

G

AI generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di esclusione

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

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. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e la rete Internet in generale.

migrazione incrementale

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

L'uso di sensori e dispositivi connessi a Internet nei settori industriali, come quello manifatturiero, energetico, automobilistico, sanitario, delle scienze della vita e dell'agricoltura. Per ulteriori

informazioni, vedere Creazione di una strategia di trasformazione digitale per l'Internet of Things (IIoT) industriale.

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

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

ramo principale

Vedi filiale.

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH.

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

Un AWS programma che fornisce consulenza, supporto, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per

eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

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

fabbrica di migrazione

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

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

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

gestione del cambiamento organizzativo (OCM)

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

Scelta indipendente della tecnologia di archiviazione di dati di un microservizio in base ai modelli di accesso ai dati e ad altri requisiti. Se i microservizi utilizzano la stessa tecnologia di archiviazione di dati, possono incontrare problemi di implementazione o registrare prestazioni

scadenti. I microservizi vengono implementati più facilmente e ottengono prestazioni e scalabilità migliori se utilizzano l'archivio dati più adatto alle loro esigenze. Per ulteriori informazioni, consulta la sezione Abilitazione della persistenza dei dati nei microservizi.

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

STRACCIO

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

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 AWSPer ulteriori informazioni, vedere Cloud AWS Resilience.

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi 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 Cosa c'è in un segreto di Secrets Manager? nella documentazione di Secrets Manager.

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

Una politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per

ulteriori informazioni, consulta le politiche di controllo del servizio nella AWS Organizations documentazione.

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

T

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

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

vulnerabilità zero-day

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

prompt zero-shot

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

applicazione zombie

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

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