Mengelola identitas dan akses untuk VMware Cloud di AWS

AWS Panduan Preskriptif

AWS Panduan Preskriptif: Mengelola identitas dan akses untuk VMware Cloud di AWS

Table of Contents

Mengelola identitas dan akses untuk VMware Cloud di AWS

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

Vern Bolinius, VMware

September 2024 (riwayat dokumen)

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

Identitas dan manajemen akses adalah prinsip membatasi akses sistem hanya untuk pengguna dan aplikasi yang berwenang, termasuk membatasi akses hanya ke sumber daya jaringan yang diperlukan. Di lingkungan cloud, kontrol manajemen identitas dan akses biasanya terdiri dari kebijakan dan layanan yang Anda gunakan untuk mengidentifikasi, mengautentikasi, dan mengotorisasi pengguna, grup pengguna, dan aplikasi.

VMware Cloud on AWS mendukung beban kerja VMware berbasis vSphere Anda di. AWS Cloud Anda dapat menggunakan banyak VMware layanan dan alat untuk mengonfigurasi, mengelola, mencadangkan, memantau, dan menganalisis infrastruktur cloud ini. Fitur dan kontrol yang Anda gunakan untuk mengelola identitas dan akses bervariasi antar layanan. Dokumen ini memberikan praktik dan rekomendasi terbaik untuk mengelola identitas dan akses untuk VMware layanan berikut:

- VMware Operasi Aria
- VMware Operasi Aria untuk Log
- VMware Operasi Aria untuk Jaringan
- VMware Cloud di AWS
- VMware Konsol Layanan Cloud
- VMware HCX
- VMware NSX
- VMware Pemulihan Cyber Langsung
- VMware Pemulihan Situs Langsung

- VMware vCenter Server

Panduan ini memberikan ikhtisar dan praktik terbaik manajemen identitas dan akses untuk VMware Cloud on AWS dan VMware layanan terkait. Ini mencakup deskripsi singkat dari setiap layanan dan membahas akses identitas dan pertimbangan manajemen untuk layanan itu. Kami juga memberikan rekomendasi untuk mengonfigurasi layanan sebagai bagian dari VMware Cloud on AWS.

> **Important**
>
> Banyak VMware layanan yang dibahas dalam panduan ini digunakan di VMware solusi cloud atau lokal lainnya. Rekomendasi dan praktik terbaik dalam panduan ini khusus untuk VMware Cloud on AWS. Rekomendasi ini mungkin tidak berlaku untuk lingkungan lain.

Audiens yang dituju

Panduan ini ditujukan untuk arsitek dan insinyur keamanan yang bertanggung jawab untuk menerapkan VMware Cloud AWS di lingkungan cloud atau hybrid mereka.

Hasil bisnis yang ditargetkan

Panduan ini membantu Anda melakukan hal berikut:

1. Memahami berbagai kontrol identitas dan manajemen akses untuk VMware Cloud on AWS dan VMware layanan terkait
2. Kenali praktik terbaik yang direkomendasikan yang membantu Anda mengoperasikan VMware Cloud dengan aman AWS
3. Memahami opsi yang tersedia untuk otentikasi federasi melalui penyedia identitas eksternal

Ikhtisar manajemen identitas

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware menggunakan konsep standar industri dan hierarki identitas berikut untuk mengelola identifikasi, otentikasi, dan otorisasi:

- Pengguna adalah individu yang mengakses lingkungan Anda dalam kapasitas tertentu. Anda dapat membuat pengguna lokal, atau Anda dapat menggunakan federasi untuk mengautentikasi pengguna dari penyedia identitas eksternal. Untuk informasi selengkapnya, lihat Federasi Identitas dan SSO.
- Grup menyediakan mekanisme untuk secara logis mengelompokkan kumpulan pengguna bersama-sama. Ini membantu Anda memberikan izin yang konsisten kepada pengguna tersebut dan mengurangi overhead administratif. Peran digunakan untuk memberikan izin kepada pengguna atau grup. Untuk informasi selengkapnya, lihat Peran dan Izin di SDDC (VMware dokumentasi).
- Organizations in VMware Cloud mengontrol akses ke satu atau beberapa VMware layanan. Pengguna dan grup harus menjadi bagian dari organisasi untuk mengakses layanan dalam organisasi. Anda dapat mengaktifkan fitur Tata Kelola Identitas dan Administrasi untuk mengizinkan identitas federasi untuk meminta keanggotaan layanan mandiri ke organisasi. VMware Untuk informasi selengkapnya, lihat VMware Konsol Layanan Cloud.

Izin dapat memberikan akses ke objek tertentu, atau mereka dapat diwarisi dari objek induk. Jika beberapa izin yang tumpang tindih ditetapkan ke pengguna atau grup, izin yang paling permisif berlaku. Untuk informasi selengkapnya, lihat Warisan Hirarkis Izin (dokumentasi)VMware .

Anda dapat menggunakan elemen struktural ini untuk mengadopsi kebijakan hak istimewa paling sedikit dan menetapkan batas akses logis dalam infrastruktur Anda berdasarkan kebutuhan pengguna. Least-privilege adalah prinsip pemberian pengguna dan aplikasi hanya akses minimum yang diperlukan untuk melakukan tugas mereka. Jika terjadi akses yang tidak sah, praktik terbaik industri ini dapat membantu membatasi kemampuan penyerang untuk menyebabkan kerusakan atau

mencuri data sensitif. Dan bahkan untuk pengguna yang berwenang, prinsip ini dapat mencegah pengguna mengakses data yang seharusnya tidak mereka miliki. Memberi pengguna akses hanya ke sumber daya yang diperlukan juga dapat meningkatkan produktivitas dan mengurangi kebutuhan akan dukungan pemecahan masalah.

Saat menggunakan VMware Cloud on AWS, ada dua layanan dan alat utama untuk mengelola identitas dan akses: VMware Konsol Layanan Cloud danVMware vCenter Server. Kemudian dalam panduan ini, kami membahas layanan ini secara lebih rinci.

Federasi Identitas dan SSO

Banyak perusahaan ingin mendirikan federasi dengan penyedia identitas eksternal (iDP). Ini memungkinkan Anda untuk memberikan pengalaman masuk tunggal (SSO) kepada pengguna Anda. Baik VMware Cloud dan vCenter Server mendukung federasi perusahaan:

- VMware Cloud mendukung Security Assertion Markup Language (SAMP) 2.0 berbasis IdPs dan mendukung Lightweight Directory Access Protocol (LDAP). Untuk informasi selengkapnya, lihat Apa itu federasi perusahaan dan cara kerjanya dengan Layanan VMware Cloud (VMware dokumentasi).
- Saat Anda mengoperasikan vCenter Server di VMware Cloud on AWS, federasi ke vCenter Server dengan menggunakan IDP eksternal saat ini tidak didukung. Hanya iDP bawaan yang dapat digunakan, yang mendukung penggunaan Microsoft Active Directory melalui LDAP. Untuk informasi selengkapnya, lihat Sumber Identitas untuk Server vCenter dengan vCenter Single Sign-On (dokumentasi). VMware

Beberapa VMware layanan terkait lainnya yang dibahas dalam panduan ini juga mendukung federasi langsung dari IDP. Namun, mengkonfigurasi federasi di setiap layanan menciptakan poin tambahan manajemen pengguna dan menjadi sulit untuk dikelola. Sebagai gantinya, Anda dapat menggunakan grup dan peran di VMware Cloud Services Console untuk menggunakan sumber identitas umum dan mengonfigurasi izin untuk layanan VMware Cloud lainnya. Selain itu, Anda dapat mengonfigurasi Mode Tertaut Hibrid untuk menggunakan identitas yang sama dengan instance Server vCenter lokal. Ini mengurangi jumlah poin federasi dan manajemen identitas menjadi dua layanan. Untuk informasi selengkapnya tentang Mode Tertaut Hibrid, lihat Mengonfigurasi Mode Tertaut Hibrid (VMware dokumentasi).

Praktik terbaik umum

Pemberitahuan

Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

Important

Banyak VMware layanan yang dibahas dalam panduan ini digunakan di VMware solusi cloud atau lokal lainnya. Rekomendasi dan praktik terbaik dalam panduan ini khusus untuk VMware Cloud on AWS. Rekomendasi ini mungkin tidak berlaku untuk lingkungan lain.

Pertimbangkan AWS rekomendasi berikut untuk mengelola identitas dan akses ke infrastruktur VMware cloud Anda:

- Terapkan kebijakan dengan hak istimewa paling sedikit. Gunakan kontrol akses berbasis peran (RBAC) untuk memberikan izin minimum dan akses yang diperlukan bagi pengguna untuk menjalankan fungsinya.
- Jika memungkinkan, berikan izin ke grup, bukan ke pengguna individu.
- Hindari mengonfigurasi pengguna lokal. Mengautentikasi pengguna terhadap penyedia identitas gabungan eksternal.
- Konfigurasikan otentikasi multi-faktor untuk semua pengguna.
- Kebijakan kata sandi Anda harus mencakup kekuatan kata sandi dan persyaratan rotasi.
- Dokumentasikan prosedur break-glass untuk mengambil kendali administratif penuh atas VMware organisasi dan layanan terkait. Breaking glass, yang menarik namanya dari memecahkan kaca untuk menarik alarm kebakaran, mengacu pada sarana bagi seseorang untuk dengan cepat mendapatkan akses administratif dalam keadaan luar biasa, dengan menggunakan proses yang disetujui dan diaudit.
- Jika Anda memiliki pusat data lokal atau beberapa instance Server vCenter, gunakan Mode Tertaut Hybrid untuk menghubungkan instance Server vCenter cloud Anda dengan domain Masuk Tunggal

vCenter lokal. Ini membantu Anda mengelola sumber daya cloud dan lokal dari satu antarmuka Klien vSphere.

- Jika memungkinkan, konfigurasikan endpoint manajemen, seperti vCenter Server, HCX Cloud Manager, dan NSX Manager, agar dapat diakses hanya dari jaringan internal, bukan dari internet publik.
- Jangan gunakan kredensi lokal, seperti akun cloudadmin, untuk tujuan administratif. Pesan akun ini untuk digunakan dalam prosedur break-glass Anda. Tindakan yang dilakukan menggunakan akun pengguna lokal administratif tidak dapat dikaitkan dengan individu tertentu, sehingga akun ini dapat digunakan untuk membuat perubahan tanpa akuntabilitas.
- Ubah kata sandi untuk akun lokal, seperti pengguna root dan administratif, ke nilai yang kuat dan simpan kredensil ini dengan aman di toko kata sandi yang diaudit. Buat proses persetujuan untuk memberikan akses ke kata sandi ini.
- Jika kredensil lokal akan bertahan untuk waktu yang lama, seperti selama beberapa bulan atau lebih, buat proses untuk memutar kredensil (misalnya, jika Anda menggunakan VMware HCX untuk meregangkan jaringan).

Rekomendasi ini berlaku untuk semua konfigurasi VMware layanan untuk VMware Cloud on AWS. Rekomendasi tambahan untuk setiap layanan dibahas nanti dalam panduan ini.

VMware layanan manajemen identitas

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

Saat menggunakan VMware Cloud on AWS, ada dua layanan dan alat utama untuk mengelola identitas dan akses: VMware Konsol Layanan Cloud danVMware vCenter Server.

VMware Konsol Layanan Cloud

VMware Cloud Services Console (VMware dokumentasi) membantu Anda mengelola portofolio layanan VMware Cloud, yang mencakup VMware Cloud on AWS. Dalam layanan ini, Anda dapat:

- Mengelola entitas, seperti pengguna dan grup
- Kelola organisasi, yang mengontrol akses ke layanan cloud lainnya, seperti VMware Live Cyber Recovery dan VMware Aria Suite
- Tetapkan peran ke sumber daya dan layanan
- Lihat OAuth aplikasi yang memiliki akses ke organisasi Anda
- Konfigurasikan federasi perusahaan untuk organisasi
- Mengaktifkan dan menerapkan layanan VMware Cloud, seperti VMware Aria dan VMware Cloud di AWS
- Kelola penagihan dan langganan
- Dapatkan VMware dukungan

Mengelola identitas dan akses

Dengan menyiapkan pengguna, grup, peran, dan organisasi dengan benar di VMware Cloud Services Console, Anda dapat menerapkan kebijakan akses hak istimewa paling sedikit.

Mengamankan akses ke VMware Cloud Services Console sangat penting karena pengguna administratif layanan ini dapat mengubah izin di seluruh lingkungan VMware cloud Anda dan

mengakses informasi sensitif, seperti informasi penagihan. Untuk mengakses semua fitur konsol, seperti penagihan dan dukungan, pengguna juga harus ditautkan dengan profil VMware Customer Connect (secara resmi dikenal sebagai My VMware).

Di VMware Cloud Services Console, Anda menggunakan jenis peran berikut untuk memberikan izin kepada pengguna dan grup:

- Peran organisasi — Peran ini berkaitan dengan organisasi VMware Cloud secara langsung, memberikan izin dalam Konsol Layanan VMware Cloud. Ada dua peran standar. Peran pemilik Organisasi memiliki izin penuh untuk mengelola organisasi. Peran anggota Organisasi memiliki akses baca ke VMware Cloud Services Console. Untuk informasi selengkapnya, lihat Peran organisasi apa yang tersedia di Layanan VMware Cloud (VMwaredokumentasi).
- Peran layanan — Peran ini memungkinkan Anda menetapkan izin untuk menggunakan layanan tertentu. Misalnya, entitas dengan peran layanan Admin DR dapat mengelola VMware Live Cyber Recovery di konsol layanan khusus. Setiap layanan yang tersedia dalam organisasi memiliki satu atau lebih peran layanan terkait. Untuk informasi lebih lanjut tentang peran layanan yang tersedia, lihat VMware dokumentasi untuk layanan yang diminati.

VMware Cloud Services Console mendukung kebijakan autentikasi. Ini dapat menetapkan bahwa pengguna harus memberikan token otentikasi kedua saat masuk, juga dikenal sebagai otentikasi multi-faktor (MFA).

Untuk informasi selengkapnya tentang mengelola identitas dan akses di layanan ini, lihat Identity and Access Management (VMware dokumentasi).

AWS rekomendasi

Selain ituPraktik terbaik umum, AWS rekomendasikan hal berikut saat mengonfigurasi VMware Cloud Services Console untuk VMware Cloud di AWS:

- Saat membuat organisasi, gunakan profil VMware Customer Connect dan alamat email perusahaan terkait yang bukan milik individu, seperti vmwarecloudroot@example.com. Akun ini harus diperlakukan sebagai layanan, atau root, akun, dan Anda harus mengaudit penggunaan dan membatasi akses ke akun email. Segera konfigurasikan federasi akun dengan penyedia identitas perusahaan (IDP) Anda sehingga pengguna dapat mengakses organisasi tanpa menggunakan akun ini. Pesan akun ini untuk digunakan dalam prosedur break-glass untuk mengatasi masalah dengan IDP federasi.

- Gunakan identitas federasi untuk organisasi untuk memberikan akses ke layanan cloud lainnya, seperti VMware Live Cyber Recovery. Jangan mengelola pengguna atau federasi secara individual di beberapa layanan. Ini menyederhanakan pengelolaan akses ke beberapa layanan, seperti ketika pengguna bergabung atau meninggalkan perusahaan.
- Tetapkan peran pemilik Organisasi dengan hemat. Entitas dengan peran ini dapat memberikan diri mereka akses penuh ke semua aspek organisasi dan layanan cloud terkait.

VMware vCenter Server

VMware vCenter Server (VMwarewebsite) adalah bidang manajemen untuk mengelola lingkungan VMware vSphere. Di vCenter Server, Anda mengelola entitas yang dapat mengakses sumber daya vSphere, seperti mesin virtual, dan mengakses add-on, seperti VMware HCX dan Live Site Recovery. VMware Anda mengelola vCenter Server melalui aplikasi VSphere Client. Di VCenter Server, Anda dapat:

- Kelola mesin virtual, VMware ESXi host, dan penyimpanan VMware vSAN
- Konfigurasikan dan kelola vCenter Single Sign-On

Jika memiliki pusat data lokal, Anda dapat menggunakan Mode Tertaut Hibrid untuk menautkan instance Server vCenter cloud ke domain Masuk Tunggal vCenter lokal. Jika domain vCenter Single Sign-On berisi beberapa instance Server vCenter yang terhubung menggunakan Enhanced Linked Mode, semua instance tersebut ditautkan ke SDDC cloud Anda. Dengan menggunakan mode ini, Anda dapat melihat dan mengelola pusat data lokal dan cloud dari satu antarmuka Klien vSphere, dan Anda dapat memigrasikan beban kerja antara pusat data lokal dan SDDC cloud. Untuk informasi selengkapnya, lihat Mengonfigurasi Mode Tertaut Hibrid (VMware dokumentasi).

Mengelola identitas dan akses

Di pusat data yang ditentukan perangkat lunak (SDDCs) (VMware situs web) untuk VMware Cloud on AWS, cara Anda mengoperasikan vCenter Server mirip dengan SDDC lokal. Perbedaan utama adalah bahwa VMware Cloud on AWS adalah layanan yang dikelola. Oleh karena VMware itu, bertanggung jawab untuk tugas-tugas administratif tertentu, seperti mengelola host, cluster, dan manajemen mesin virtual. Untuk informasi selengkapnya, lihat Apa yang Berbeda di Cloud? dan Izin global (VMware dokumentasi).

Karena VMware melakukan beberapa tugas administratif untuk SDDC, administrator cloud memerlukan lebih sedikit hak istimewa daripada administrator pusat data lokal. Saat Anda membuat

VMware Cloud di AWS SDDC, pengguna cloudadmin secara otomatis dibuat dan ditetapkan CloudAdminperan (dokumentasi). VMware Anda dapat menggunakan akun pengguna lokal istimewa ini untuk mengakses vCenter Server dan vCenter Single Sign-On. Pengguna yang memiliki peran layanan VMware Cloud on AWS Administrator atau Administrator (Delete Restricted) di VMware Cloud Services Console dapat memperoleh kredensialnya untuk pengguna cloudadmin. CloudAdminPeran ini memiliki izin maksimum yang mungkin di vCenter Server untuk Cloud AWS di VMware SDDC. Untuk informasi selengkapnya tentang peran layanan ini, lihat CloudAdmin Hak Istimewa (VMware dokumentasi). Pengguna cloudadmin adalah satu-satunya pengguna lokal yang tersedia untuk vCenter Server di Cloud on. VMware AWS Untuk memberikan akses bagi pengguna lain, gunakan sumber identitas eksternal.

vCenter Single Sign-On adalah broker otentikasi yang menyediakan infrastruktur pertukaran token keamanan. Ketika pengguna mengautentikasi ke vCenter Single Sign-On, pengguna tersebut menerima token yang dapat digunakan untuk mengautentikasi dengan vCenter Server dan layanan add-on lainnya dengan menggunakan panggilan API. Pengguna cloudadmin dapat mengonfigurasi sumber identitas eksternal untuk vCenter Server. Untuk informasi selengkapnya, lihat Sumber Identitas untuk Server vCenter dengan vCenter Single Sign-On (dokumentasi). VMware

Di VCenter Server, Anda menggunakan tiga jenis peran berikut untuk memberikan izin kepada pengguna dan grup:

- Peran sistem — Anda tidak dapat mengedit atau menghapus peran ini.
- Contoh peran — Peran ini mewakili kombinasi tugas yang sering dilakukan. Anda dapat menyalin, mengedit, atau menghapus peran ini.
- Peran kustom - Jika sistem dan contoh peran tidak menyediakan kontrol akses yang Anda inginkan, Anda dapat membuat peran kustom di Klien vSphere. Anda dapat menduplikasi dan memodifikasi peran yang ada, atau Anda dapat membuat peran baru. Untuk informasi selengkapnya, lihat Membuat Peran Kustom Server vCenter (VMware dokumentasi).

Untuk setiap objek dalam inventaris SDDC, Anda hanya dapat menetapkan satu peran ke pengguna atau grup. Jika, untuk satu objek, pengguna atau grup memerlukan kombinasi peran bawaan, ada dua opsi. Opsi pertama adalah membuat peran khusus dengan izin yang diperlukan. Opsi lainnya adalah membuat dua grup, menetapkan peran bawaan untuk masing-masing, dan kemudian menambahkan pengguna ke kedua grup.

AWS rekomendasi

Selain ituPraktik terbaik umum, AWS merekomendasikan hal berikut saat mengkonfigurasi vCenter Server VMware untuk Cloud on: AWS

- Gunakan akun pengguna cloudadmin untuk mengonfigurasi sumber identitas eksternal di vCenter Single Sign-On. Tetapkan pengguna yang sesuai dari sumber identitas eksternal yang akan digunakan untuk tujuan administratif, dan kemudian hentikan penggunaan pengguna cloudadmin. Untuk praktik terbaik saat mengonfigurasi vCenter Single Sign-On, lihat Keamanan Informasi dan Akses untuk Server vCenter (dokumentasi). VMware
- Di VSphere Client, perbarui kredensi cloudadmin untuk setiap instance Server vCenter ke nilai baru, lalu simpan dengan aman. Perubahan ini tidak tercermin di VMware Cloud Services Console. Misalnya, melihat kredensional melalui Cloud Services Console menunjukkan nilai asli.

  > **Note**
  >
  > Jika kredensi untuk akun ini hilang, VMware dukungan dapat mengatur ulang mereka.

- Jangan gunakan akun cloudadmin untuk day-to-day akses. Pesan akun ini untuk digunakan sebagai bagian dari prosedur break-glass.
- Batasi akses jaringan ke vCenter Server hanya untuk jaringan pribadi.

VMware Layanan terkait

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

Bab ini memberikan praktik dan rekomendasi terbaik untuk mengelola identitas dan akses untuk VMware layanan berikut yang terkait dengan VMware Cloud on AWS:

- Layanan yang dikelola melalui VMware Cloud Services Console:
  - VMware Awan di AWS
  - VMware NSX
  - VMware Operasi Aria untuk Log
  - VMware Operasi Aria untuk Jaringan
  - VMware Operasi Aria
  - VMware Pemulihan Cyber Langsung
- Layanan dikelola melalui VMware vCenter Server:
  - VMware HCX
  - VMware Pemulihan Situs Langsung

Panduan ini memberikan deskripsi singkat tentang setiap layanan, membahas akses identitas dan kontrol manajemen untuk layanan tersebut, dan mencakup AWS rekomendasi untuk mengonfigurasi layanan tersebut sebagai bagian dari VMware Cloud on. AWS

VMware Awan di AWS

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware Cloud on AWS (VMware dokumentasi) adalah layanan yang dirancang bersama oleh AWS dan VMware untuk membantu Anda memigrasi dan memperluas lingkungan berbasis VMware vSphere lokal Anda ke. AWS Cloud

Anda dapat mengakses VMware Cloud AWS melalui VMware Cloud Services Console, jika Anda termasuk dalam organisasi yang memberikan akses ke layanan ini. Di VMware Cloud on AWS, Anda dapat:

- Buat dan hapus SDDCs.
- Mengelola kelompok SDDC.
- Mengelola SDDCs, termasuk jaringan dan parameter cluster.
- Akses kredensi pengguna cloudadmin untuk VMware vCenter Server. Untuk informasi lebih lanjut tentang pengguna ini, lihat VMware vCenter Server di panduan ini.
- Akses kredensi pengguna cloud_admin untuk NSX. VMware Untuk informasi lebih lanjut tentang pengguna ini, lihat VMware NSX di panduan ini.
- Aktifkan dan terapkan layanan add-on di dalamnya SDDCs, seperti VMware Live Site Recovery dan VMware HCX.
- Akses konsol untuk layanan add-on, termasuk HCX dan VMware Live Site Recovery.

Mengelola identitas dan akses

Anda menggunakan VMware Cloud Services Console untuk mengelola identitas dan akses ke VMware Cloud. AWS Untuk VMware Cloud on AWS, peran layanan berikut tersedia:

- Administrator — Peran ini memiliki akses penuh ke VMware Cloud on AWS.
- Administrator (Hapus Terbatas) — Peran ini memiliki akses penuh ke VMware Cloud on AWS, tidak termasuk operasi penghapusan SDDC.
- Admin Awan NSX
- Auditor Cloud NSX

> **Note**
>
> NSX Cloud Admin dan NSX Cloud Auditor terkait dengan penggunaan NSX. VMware Untuk informasi selengkapnya, lihat VMware NSX.

Salah satu dari dua peran Administrator diperlukan untuk mengakses SDDC dalam Cloud Services Portal. Pengguna tanpa salah satu dari dua peran Cloud NSX tidak dapat mengakses tab Jaringan dan Keamanan SDDC dalam Portal Layanan Cloud, selain itu mereka tidak dapat mengakses kredenal admin NSX.

AWS rekomendasi

Selain ituPraktik terbaik umum, AWS rekomendasikan hal berikut saat mengonfigurasi VMware Cloud di AWS:

- Untuk memberikan penilaian kepada administrator, gunakan hanya peran Administrator (Hapus Dibatasi). Cadangan peran Administrator untuk akses break-glass saat Anda perlu menghapus SDDC.
- Jangan berikan peran NSX kepada pengguna yang tidak memerlukan akses ke konfigurasi jaringan dan firewall. Untuk informasi selengkapnya, lihat VMware NSX dalam panduan ini.
- Ubah kata sandi untuk akun pengguna lokal cloudadmin ke nilai yang kuat dan simpan kredensil ini dengan aman di penyimpanan kata sandi yang diaudit. Anda dapat mengubah kata sandi ini di VMware vCenter Server dengan menggunakan VSphere Web Client.

VMware NSX

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra saluran nya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware NSX (VMwaredokumentasi) menyediakan lapisan virtualisasi jaringan yang mereproduksi model Open Systems Interconnection (OSI) dari lapisan 2 hingga lapisan 7; dengan fitur termasuk switching, routing, dan firewall. Ada dua versi NSX. Versi asli (NSX-V) mengharuskan Anda juga menyebarkan vCenter Server. Versi yang lebih baru (NSX-T) dipisahkan dari vCenter Server, yang memungkinkan dukungan untuk arsitektur hybrid. VMware Cloud on AWS menggunakan NSX-T.

NSX, bersama dengan vSphere dan vSAN, adalah komponen inti dari Cloud on. VMware AWS NSX menyediakan semua fungsi jaringan dalam SDDC dan mengelola interaksi antara jaringan overlay dan komponen AWS asli yang membentuk underlay jaringan. NSX erat digabungkan dengan layanan

lain, seperti vCenter Server dan VMware HCX, yang memanggil NSX untuk mengelola sumber daya. APIs

Di NSX, Anda dapat:

- Mengelola switching dan routing
- Mengelola firewall, termasuk menggunakan firewall terdistribusi untuk inspeksi inline antara VMs atau antara jaringan dan internet publik
- Mengelola jaringan pribadi virtual (VPNs)
- Konfigurasikan Protokol Konfigurasi Host Dinamis (DHCP) dan Sistem Nama Domain (DNS)

Anda dapat mengakses NSX dari VMware Cloud Services Console atau melalui antarmuka pengguna web (UI) NSX Manager khusus. UI web NSX Manager menawarkan beberapa fitur tambahan yang tidak tersedia di VMware Cloud Services Console. Untuk informasi selengkapnya, lihat Administrasi Jaringan SDDC dengan Manajer NSX (dokumentasi)VMware .

Perhatikan hal berikut saat mengakses NSX di VMware Cloud on: AWS

- Untuk mengakses NSX melalui VMware Cloud Services Console, Anda harus diberi peran VMware Cloud on AWS Administrator. Anda dapat mengakses NSX di tab Jaringan dan Keamanan SDDC. Untuk informasi lebih lanjut tentang peran ini, lihat VMware Awan di AWS di panduan ini.
- Anda dapat membuka UI web Manajer NSX dengan memilih tautan pada tab Pengaturan SDDC atau dengan memilih Buka Manajer NSX di halaman Ringkasan SDDC. Untuk informasi selengkapnya, lihat Buka Manajer NSX (VMware dokumentasi).
- Jika SDDC dalam mode Payment Card Industry Data Security Standard (PCI DSS), Anda tidak dapat mengakses NSX melalui tab Networking and Security di Cloud Services Console. VMware Anda harus menggunakan UI web NSX Manager.

Mengelola identitas dan akses

Anda menggunakan VMware Cloud Services Console untuk mengelola identitas dan akses ke VMware NSX. Untuk NSX di VMware Cloud on AWS, peran layanan berikut tersedia:

- NSX Cloud Admin — Peran ini dapat mengelola fungsionalitas VMware NSX dengan VMware Cloud on. AWS
- NSX Cloud Auditor — Peran ini dapat melihat pengaturan dan acara layanan NSX tetapi tidak dapat membuat perubahan apa pun.

> **Note**
>
> Terlepas dari nama mereka, peran ini tidak terkait dengan layanan VMware NSX Cloud.

Pengguna berikut dapat mengakses NSX:

- Pengguna lokal cloud_admin, yang merupakan pengguna NSX lokal bawaan dan sangat istimewa. Pengguna yang memiliki peran Admin Cloud NSX dapat mengakses kredensil untuk akun pengguna ini. Meskipun nama mereka mirip, pengguna cloud_admin berbeda dari pengguna lokal cloudadmin@vmc.local vCenter Single Sign-On.
- Pengguna yang telah diberi peran layanan NSX Cloud Admin atau peran layanan NSX Cloud Auditor di VMware Cloud Services Console. Pengguna ini bisa menjadi pengguna VMware Cloud Services Console atau pengguna gabungan eksternal.
- Pengguna yang telah langsung diberikan akses ke NSX dari sumber identitas melalui LDAP.

AWS rekomendasi

Selain ituPraktik terbaik umum, AWS rekomendasikan hal berikut saat mengonfigurasi NSX untuk VMware Cloud di: AWS

- Jika perusahaan Anda memiliki pengguna yang bertanggung jawab untuk mengelola jaringan dan firewall tetapi tidak bertanggung jawab untuk mengelola SDDCs, berikan pengguna ini salah satu peran NSX, tetapi jangan beri mereka peran Administrator. Pengguna ini harus mengakses NSX melalui UI web NSX Manager.
- Ubah kata sandi untuk akun pengguna lokal cloud_admin ke nilai yang kuat dan simpan kredensil ini dengan aman di penyimpanan kata sandi yang diaudit. Untuk mengubah kata sandi ini, Anda harus menghubungi VMware dukungan.
- Hindari pemberian akses ke pengguna eksternal secara langsung di dalam NSX. Sebagai gantinya, siapkan federasi perusahaan di VMware Cloud Services Console, lalu gunakan peran dan grup untuk memberikan akses ke layanan ini.

VMware Operasi Aria untuk Log

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware Aria Operations for Logs (VMware dokumentasi), sebelumnya VMwarevRealize Log Insight Cloud, adalah alat penyimpanan dan analisis log yang membantu Anda memvisualisasikan dan menanyakan data log yang dihasilkan oleh Anda. VMware SDDCs Dalam Operasi VMware Aria untuk Log, Anda dapat:

- Integrasikan dengan instance Operasi vRealize lokal
- Mengumpulkan dan menganalisis semua jenis data log yang dihasilkan mesin
- Konfigurasikan peringatan
- Memantau dan menganalisis log dari VMware layanan lain

Ada dua versi layanan manajemen log terpusat ini. VMware vRealize Log Insight adalah versi lokal yang dapat berjalan sebagai alat dalam SDDC Anda. VMware Operasi Aria untuk Log adalah versi software-as-a-service (SaaS). VMware Cloud on AWS menggunakan versi cloud sebagai layanan logging default, dan ini tidak dapat diubah. Jika menggunakan versi lokal, Anda harus meneruskan log dari instans cloud ke instans lokal.

VMware Operasi Aria untuk Log disertakan dengan VMware Cloud on AWS. Versi yang disertakan memiliki kapasitas konsumsi terbatas dan periode retensi penyimpanan. Jika perlu, Anda dapat meningkatkan ke langganan premium untuk meningkatkan batas ini. Untuk informasi selengkapnya, lihat Langganan dan Penagihan (VMware dokumentasi).

Mengelola identitas dan akses

Anda menggunakan VMware Cloud Services Console untuk mengelola identitas dan akses ke Operasi VMware Aria untuk Log. VMware Operasi Aria untuk Log menggunakan pengguna yang sama, termasuk identitas gabungan, dan grup yang Anda konfigurasikan di VMware Cloud Services Console. Untuk memberikan izin untuk layanan ini, Anda dapat menetapkan peran layanan atau

mengonfigurasi peran kustom dalam Operasi VMware Aria untuk Log. Untuk informasi selengkapnya, lihat Peran Layanan (VMware dokumentasi).

VMware vRealize Log Insight memiliki dua peran default. Peran Administrator memiliki akses dan kontrol penuh, dan peran Pengguna memiliki akses baca dan dapat membuat dasbor. Anda dapat menggunakan peran khusus untuk memberikan akses ke hanya kumpulan data tertentu. Kumpulan data ini berisi filter yang membatasi data log mana yang tersedia bagi pengguna. Untuk informasi selengkapnya, lihat Membuat Kumpulan Data (VMware dokumentasi).

AWS rekomendasi

Patuhi yang Praktik terbaik umum dijelaskan sebelumnya dalam panduan ini. Kami tidak memiliki rekomendasi tambahan untuk mengelola identitas dan akses dalam layanan ini.

VMware Operasi Aria untuk Jaringan

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra saluran nya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware Aria Operations for Networks, sebelumnya VMware vRealize Network Insight Cloud, adalah versi SaaS dari vRealize Network Insight. VMware VRealize Network Insight (VMware dokumentasi) membantu Anda memahami arus lalu lintas untuk beban kerja Anda. Anda dapat menggunakan layanan ini untuk mendiagnosis masalah jaringan dan memodelkan aturan firewall untuk mendukung segmentasi beban kerja. Dalam Operasi VMware Aria untuk Jaringan, Anda dapat:

- Lihat lingkungan hybrid dan multi-cloud Anda
- Memecahkan masalah dan menganalisis dan arus lalu lintas
- Menemukan dan menganalisis aplikasi
- Memetakan dependensi antar beban kerja

Ada tiga versi layanan ini. VMware VRealize Network Insight adalah sebuah on-premises-only versi. VMware Aria Operations for Networks adalah versi SaaS. vRealize Network Insight Universal dapat

digunakan sebagai solusi lokal atau sebagai solusi SaaS cloud federasi. Semua versi kompatibel dengan VMware Cloud on AWS.

Mengelola identitas dan akses

Anda menggunakan VMware Cloud Services Console untuk mengelola identitas dan akses ke Operasi VMware Aria untuk Jaringan. VMware Operasi Aria untuk Jaringan menggunakan pengguna yang sama, termasuk identitas gabungan, dan grup yang Anda konfigurasikan di VMware Cloud Services Console. Untuk Operasi VMware Aria untuk Jaringan, peran layanan berikut tersedia:

- Administrator — Peran ini memiliki akses dan kontrol penuh.
- Anggota — Peran ini memiliki akses terbatas.
- Auditor — Peran ini memiliki akses hanya-baca.

AWS rekomendasi

Patuhi yang Praktik terbaik umum dijelaskan sebelumnya dalam panduan ini. Kami tidak memiliki rekomendasi tambahan untuk mengelola identitas dan akses dalam layanan ini.

VMware Operasi Aria

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra saluran nya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware Aria Operations (VMware dokumentasi), sebelumnya VMware vRealize Operations Cloud, adalah platform manajemen operasi untuk VMware Cloud on. AWS Layanan ini menggunakan kecerdasan buatan dan pembelajaran mesin (AI/ML) untuk membantu Anda mengoptimalkan, merencanakan, dan menskalakan aplikasi dan infrastruktur dalam penyebaran cloud hybrid Anda. Dalam Operasi VMware Aria, Anda dapat:

- Lihat rekomendasi pengoptimalan bertenaga AI/ML untuk kinerja dan kapasitas
- Manajemen kepatuhan dan konfigurasi sumber daya

- Akses alat untuk membantu Anda memecahkan masalah, seperti menyelesaikan masalah pelanggan atau menanggapi peringatan
- Gunakan paket manajemen (VMware dokumentasi) untuk memperluas fitur pemantauan, pemecahan masalah, dan remediasi layanan ini

Ada dua versi dari layanan manajemen operasi ini. VMware VRealize Operations adalah versi lokal yang dapat berjalan sebagai alat dalam SDDC Anda. VMware Aria Operations adalah versi software-as-a-service (SaaS) dari VRealize Operations. Kedua versi kompatibel dengan VMware Cloud on AWS. Karena VMware Cloud on AWS adalah layanan terkelola dan akses ke beberapa sumber daya dibatasi, tidak semua fitur Operasi vRealize didukung. Untuk informasi selengkapnya, lihat Batasan Diketahui (VMware dokumentasi).

Mengelola identitas dan akses

Anda menggunakan VMware Cloud Services Console untuk mengelola identitas dan akses ke Operasi VMware Aria. VMware Operasi Aria menggunakan pengguna yang sama, termasuk identitas gabungan, yang Anda konfigurasikan di VMware Cloud Services Console. Untuk memberikan izin untuk layanan ini, Anda dapat menetapkan peran layanan atau mengonfigurasi peran kustom dalam Operasi VMware Aria. Untuk informasi selengkapnya tentang peran layanan yang tersedia, lihat Peran dan Hak Istimewa (VMware dokumentasi).

Ada tiga peran bawaan: Administrator, GeneralUserdan ReadOnly, dan jika diperlukan, Anda dapat membuat peran khusus agar sesuai dengan persyaratan izin tertentu. Anda dapat membuat grup untuk meminimalkan overhead administratif mengelola izin untuk beberapa pengguna.

Versi lokal Operasi VMware vRealize mendukung pengguna lokal, dan versi cloud dan lokal mendukung pengguna gabungan. Namun, federasi pengguna ke penyedia identitas eksternal bervariasi antara operasi vRealize versi lokal dan cloud. Untuk versi lokal, Anda dapat langsung mengfederasi pengguna dari IDP eksternal melalui LDAP, atau Anda dapat menggunakan identitas yang Anda federasi di vCenter Server. Untuk versi cloud, Anda menggunakan pengguna yang sama, termasuk pengguna federasi, yang Anda konfigurasikan di VMware Cloud Services Console.

AWS rekomendasi

Selain ituPraktik terbaik umum, AWS rekomendasikan hal berikut saat mengonfigurasi Operasi VMware Aria untuk VMware Cloud di AWS:

- Hindari federasi pengguna secara langsung. Untuk versi cloud, gabungkan pengguna di VMware Cloud Services Console, lalu gunakan peran dan grup untuk memberikan akses ke layanan ini. Untuk versi lokal layanan ini, gunakan identitas dari sumber yang diautentikasi atau aktifkan sistem masuk tunggal (SSO). Untuk informasi selengkapnya, lihat Sumber otentikasi dan Mengonfigurasi Sumber Masuk Tunggal (dokumentasi)VMware .

VMware Pemulihan Cyber Langsung

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware Live Cyber Recovery (VMware dokumentasi) adalah pemulihan bencana sebagai solusi layanan (DRaaS) yang memberikan pendekatan berjenjang untuk pemulihan bencana. Anda dapat menyesuaikan biaya dan rentang waktu untuk tujuan titik pemulihan (RPO) dan tujuan waktu pemulihan (RTO) Anda untuk memenuhi persyaratan untuk beban kerja tertentu. Ini membantu Anda menyeimbangkan perlindungan yang andal dan penggunaan sumber daya pemulihan bencana yang efisien. Dalam VMware Live Cyber Recovery, Anda dapat:

- Buat cadangan mesin virtual
- Simpan cadangan di penyimpanan cloud yang tahan lama
- Pilih antara opsi penerapan fleksibel untuk target restorasi, dari sesuai permintaan hingga siaga panas
- Konfigurasikan kustom RPOs dan RTOs

Mengelola identitas dan akses

Anda menggunakan VMware Cloud Services Console untuk mengelola identitas dan akses ke VMware Live Cyber Recovery. VMware Live Cyber Recovery menggunakan pengguna yang sama, termasuk identitas gabungan, dan grup yang Anda konfigurasikan di VMware Cloud Services Console. Untuk memberikan izin untuk layanan ini, Anda dapat menetapkan peran layanan VMware Live Cyber Recovery atau membuat peran khusus dalam VMware Live Cyber Recovery. Untuk

informasi selengkapnya tentang peran layanan yang tersedia, lihat Peran pengguna akhir Pemulihan Siber VMware Langsung (VMware dokumentasi).

VMware Live Cyber Recovery mencakup beberapa peran bawaan yang dapat Anda gunakan untuk mengoperasikan layanan:

- Administrator — Kontrol penuh, tidak termasuk akses ke token API.
- Auditor — Akses hanya-baca ke antarmuka pengguna, tidak termasuk manajemen pengguna. Akses ke laporan kepatuhan.
- DR Admin — Membuat, menguji, dan menjalankan rencana pemulihan bencana.
- Backup Admin - Kelola situs yang dilindungi dan grup perlindungan. Akses untuk memulihkan VMs.
- Plan Tester - Buat rencana pemulihan bencana, jalankan pemulihan uji.
- Admin SDDC - Kelola. SDDCs

AWS rekomendasi

Patuhi yang Praktik terbaik umum dijelaskan sebelumnya dalam panduan ini. Kami tidak memiliki rekomendasi tambahan untuk mengelola identitas dan akses dalam layanan ini.

VMware HCX

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware HCX (VMwaredokumentasi) adalah platform mobilitas aplikasi yang memungkinkan migrasi beban kerja antar. SDDCs VMware HCX disertakan dengan VMware Cloud on AWS dan dapat digunakan untuk memigrasikan beban kerja. Di VMware HCX, Anda dapat:

- Konfigurasikan jerat multi-situs antara SDDCs
- Memperluas jaringan antara situs HCX
- Migrasikan mesin virtual

Mengelola identitas dan akses

Anda menggunakan VMware vCenter Server untuk mengelola identitas dan akses ke HCX. VMware VMware HCX memerlukan akses ke VMware layanan lain untuk membuat dan mengelola sumber daya dan migrasi, termasuk akses ke vCenter Server dan NSX. VMware HCX memiliki dua layanan komponen:

- HCX Cloud Manager — Di VMware Cloud Services Console, Anda mengaktifkan VMware HCX untuk SDDC. Ini menginstal alat HCX Cloud Manager dalam SDDC yang dipilih. Untuk informasi selengkapnya, lihat Menyebarkan OVA Penginstal HCX di Klien vSphere (dokumentasi). VMware Setelah penerapan, Anda dapat menggunakan kredensyal cloudadmin vCenter Server untuk mengakses layanan HCX Cloud Manager.
- Konektor HCX - Anda dapat memperoleh file HCX Connector Open Virtualization Archive (OVA) melalui layanan HCX Cloud Manager. Anda menggunakan file ini untuk menginstal alat HCX Cloud Manager pada instance Server vCenter apa pun, yang menyiapkan instance tersebut sebagai sumber migrasi di HCX. VMware Setiap instans Konektor HCX memiliki kredensialnya sendiri admin dan root.

Setelah Anda menerapkan kedua layanan komponen, Anda dapat mengakses VMware HCX melalui vCenter Server. Grup Administrator vCenter Single Sign-On secara otomatis diberikan peran Administrator HCX. Instalasi HCX menambahkan banyak peran tambahan dan hak istimewa untuk vCenter Single Sign-On. Gunakan ini untuk membuat kontrol akses berbutir halus untuk VMware HCX, berdasarkan berbagai jenis pengguna.

AWS rekomendasi

Selain ituPraktik terbaik umum, AWS rekomendasikan hal berikut saat mengonfigurasi VMware HCX untuk VMware Cloud di: AWS

- Gunakan aturan Gateway Firewall untuk membatasi akses jaringan ke layanan HCX Cloud Manager.
- Simpan dengan aman admin Konektor HCX lokal dan kredenal pengguna root. Pertimbangkan untuk memutar kredensil ini sesuai dengan kebijakan perusahaan Anda. VMware mengelola kredensitas ini atas nama Anda untuk HCX Cloud Manager.
- Untuk instans Konektor HCX lokal, pertimbangkan untuk membuat peran HCX kustom yang sesuai dengan kebutuhan berbagai jenis pengguna HCX Anda. Misalnya, buat peran yang lebih permisif

bagi pengguna yang mengatur dan mengelola HCX, dan buat peran yang kurang permisif bagi pengguna yang hanya mengelola migrasi.

- Saat memasangkan VMware HCX dengan VMware Cloud aktif AWS, Anda harus menggunakan pengguna cloudadmin.
- Saat memasangkan HCX Cloud dengan VMware Cloud on AWS, autentikasi tidak didukung antara VMware Cloud di AWS SDDC dan Active Directory. Untuk informasi selengkapnya, lihat [VMC on AWS] AD tidak didukung untuk penyiapan HCX Cloud to Cloud (VMware Knowledge Base article 90433).

VMware Pemulihan Situs Langsung

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

VMware Live Site Recovery (VMware dokumentasi) adalah solusi pemulihan bencana sesuai permintaan sebagai layanan (DRaaS) yang didasarkan pada layanan Manajer Pemulihan VMware Situs untuk lingkungan lokal. Dalam VMware Live Site Recovery, Anda dapat:

- Menerapkan replikasi, orkestrasi, dan otomatisasi untuk membantu melindungi beban kerja jika terjadi kegagalan situs
- Buat solusi pemulihan end-to-end bencana untuk membantu melindungi SDDCs

Mengelola identitas dan akses

Anda menggunakan VMware vCenter Server untuk mengelola identitas dan akses ke VMware Live Site Recovery. VMware Live Site Recovery melakukan operasi atas nama pengguna, seperti mereplikasi atau mematikan mesin virtual. VMware Live Site Recovery menggunakan peran dan hak istimewa untuk membantu memastikan bahwa hanya pengguna dengan izin yang benar yang dapat melakukan operasi pemulihan, seperti menjalankan semua langkah dalam rencana pemulihan.

Untuk informasi selengkapnya, lihat Hak Istimewa, Peran, dan Izin Pemulihan Situs VMware Langsung (VMware dokumentasi).

Jika Anda menggunakan identitas federasi untuk mengakses vCenter Server, Anda harus menggunakan Mode Tertaut Hybrid untuk menambahkan entitas ke grup ini. Untuk informasi selengkapnya, lihat Mengonfigurasi Mode Tertaut Hibrid (VMware dokumentasi).

AWS rekomendasi

Selain ituPraktik terbaik umum, AWS rekomendasikan hal berikut saat mengonfigurasi VMware Live Site Recovery untuk VMware Cloud di AWS:

- Pastikan pengguna diberi peran yang sama di situs sumber dan target. Ini memastikan bahwa objek yang dilindungi dan dipulihkan memiliki izin yang identik.
- Gunakan Hybrid Linked Mode untuk mengelola penetapan peran untuk identitas federasi dalam vCenter Server.
- VMware Live Site Recovery menggunakan alamat IP pribadi hanya dalam SDDC. Sejalan dengan ituPraktik terbaik umum, pastikan bahwa VMware Cloud Anda di AWS vCenter menyelesaikan ke alamat IP pribadi.

Contoh kelompok dan peran

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

Tabel berikut memberikan contoh strategi manajemen identitas dan akses untuk menggunakan VMware Cloud on AWS. Ini menguraikan persona pengguna, VMware layanan yang perlu diakses oleh persona, keanggotaan organisasi dan grup, peran yang diberikan, dan jenis identitas yang digunakan (seperti pengguna lokal atau identitas federasi). Dengan menggunakan tabel ini sebagai titik awal, rancang strategi untuk perusahaan Anda yang mematuhi praktik terbaik yang direkomendasikan dalam panduan ini.

Persona pengguna	Layanan diakses	VMware Nama grup sampel cloud	VMware Peran layanan cloud	vCenter Single Sign-On nama grup sampel	Peran Masuk Tunggal vCenter	Sumber identitas
Organisasi memecahkan kaca	VMware Konsol Layanan Cloud	Tidak ada	Pemilik organisasi	Tidak ada	Tidak ada	Pengguna lokal (alamat email akun layanan)
VMware administrator	VMware Konsol Layanan Cloud vCenter Server HCX	`vmware_admins`	Pemilik organisasi	`vmware_admins`	Administrator	Penyedia identitas federasi

Persona pengguna	Layanan diakses	VMware Nama grup sampel cloud	VMware Peran layanan cloud	vCenter Single Sign-On nama grup sampel	Peran Masuk Tunggal vCenter	Sumber identitas
	VMware Pemulihan Situs Langsung VMware Pemulihan Cyber Langsung Operasi VRealize					
Administrator cadangan	vCenter Server	Tidak ada	Tidak ada	`vmware_backups`	Pengguna daya	Penyedia identitas federasi

Persona pengguna	Layanan diakses	VMware Nama grup sampel cloud	VMware Peran layanan cloud	vCenter Single Sign-On nama grup sampel	Peran Masuk Tunggal vCenter	Sumber identitas
Administrator pemulihan bencana	vCenter Server VMware Konsol Layanan Cloud VMware Pemulihan Situs Langsung VMware Pemulihan Cyber Langsung	`vmware_dr`	Anggota organisasi DR Admin DR SDDC Admin	`vmware_dr`	SrmAdministrator HmsCloudAdmin	Penyedia identitas federasi
VMware operator	VMware Konsol Layanan Cloud vCenter Server HCX Operasi VRealize	`vmware_ops`	Anggota organisasi v ROps Administrator	`vmware_ops`	Pengguna daya	Penyedia identitas federasi

Persona pengguna	Layanan diakses	VMware Nama grup sampel cloud	VMware Peran layanan cloud	vCenter Single Sign-On nama grup sampel	Peran Masuk Tunggal vCenter	Sumber identitas
Tim jaringan	VMware Konsol Layanan Cloud vCenter Server	`vmware_networks`	Anggota organisasi Admin Awan NSX	`vmware_networks`	Hanya baca	Penyedia identitas federasi
Tim keamanan	VMware Konsol Layanan Cloud vCenter Server HCX (akses sementara) VMware Pemulihan Situs Langsung VMware Pemulihan Cyber Langsung Operasi VRealize	`vmware_security`	Anggota organisasi v ROps ReadOnly	`vmware_security`	Hanya baca	Penyedia identitas federasi

Persona pengguna	Layanan diakses	VMware Nama grup sampel cloud	VMware Peran layanan cloud	vCenter Single Sign-On nama grup sampel	Peran Masuk Tunggal vCenter	Sumber identitas
Auditor	VMware Konsol Layanan Cloud vCenter Server	`vmware_audit`	Anggota organisasi	`vmware_audit`	Hanya baca	Penyedia identitas federasi

Langkah selanjutnya

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

Panduan ini mencakup praktik terbaik yang kami rekomendasikan untuk mengelola identitas dan akses untuk VMware Cloud di AWS dan VMware layanan terkait. Rekomendasi ini dirancang untuk membantu Anda mengamankan infrastruktur cloud dan cloud hybrid Anda serta mencegah akses yang tidak sah, tetapi mereka juga dirancang agar dapat diskalakan dan efisien. Dengan menetapkan pengguna ke grup dan kemudian menetapkan peran ke grup, Anda dapat lebih cepat memberikan atau membatasi izin dan meminimalkan biaya overhead yang terkait dengan mengonfigurasi pengguna secara individual. Selain itu, dengan menggunakan federasi ke penyedia identitas eksternal dan vCenter Single Sign-On, Anda dapat memberikan pengalaman masuk tunggal yang mulus kepada pengguna Anda.

Gunakan Contoh kelompok dan peran tabel untuk mulai merancang strategi manajemen identitas dan akses yang sesuai untuk perusahaan Anda. Setelah Anda meninjau rekomendasi dalam panduan ini, kami sarankan Anda meninjau tautan yang disediakan di Sumber daya bagian ini. Sumber daya ini akan membantu Anda mempelajari lebih lanjut tentang layanan VMware Cloud dan cara mengonfigurasi praktik terbaik yang dijelaskan dalam panduan ini.

Sumber daya

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

AWS Sumber daya terkait

- VMware Cloud pada AWS ikhtisar dan model operasi
- Opsi pemulihan bencana untuk beban kerja di VMware Cloud di AWS
- Mengonfigurasi opsi penyimpanan offload untuk VMware Cloud on AWS
- Menerapkan VMware SDDC AWS dengan menggunakan Cloud di VMware AWS
- Migrasi VMware SDDC ke VMware Cloud saat menggunakan HCX AWS VMware

VMware dokumentasi

VMware Awan di AWS

- Menyiapkan Federasi Perusahaan untuk Layanan Cloud
- VMware Identitas dan Access Management Layanan Cloud

VMware vCenter Server dan vCenter Single Sign-On

- Memahami Otorisasi di vSphere
- Administrasi vSphere di VMware Cloud on AWS
- Otentikasi vSphere dengan vCenter Single Sign-On
- Mengkonfigurasi Sumber Identitas Masuk Tunggal vCenter
- Warisan Hirarkis Izin
- Keamanan Informasi dan Akses untuk VCenter Server
- VSphere Diperlukan Hak Istimewa untuk Tugas Umum

VMware NSX

- Panduan Administrasi NSX
- Keamanan Informasi dan Akses untuk Pusat Data NSX-T

VMware HCX

- VMware Dokumentasi HCX
- VMware Akun Pengguna HCX dan Persyaratan Peran

VMware Aria dan vRealize suite

- VMware Dokumentasi Operasi VRealize
- Peran dan Hak Istimewa di VRealize Operations Cloud
- VMware Lembar Data Wawasan Log VRealize
- Memulai Operasi VMware Aria untuk Log
- VMware Dokumentasi Layanan Cloud
- Manajemen Pengguna VRealize Network Insight

VMware Pemulihan Situs Langsung

- VMware Dokumentasi Pemulihan Situs Langsung
- VMware Hak Istimewa, Peran, dan Izin Pemulihan Situs Langsung

VMware Pemulihan Cyber Langsung

- VMware Dokumentasi Pemulihan Cyber Langsung
- VMware Peran Pengguna Akhir Pemulihan Cyber Langsung

Riwayat dokumen

> **Pemberitahuan**
>
> Per 30 April 2024, VMware Cloud on AWS tidak lagi dijual kembali oleh AWS atau mitra salurannya. Layanan ini akan terus tersedia melalui Broadcom. Kami mendorong Anda untuk menghubungi AWS perwakilan Anda untuk detailnya.

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
VMware penawaran layanan	Kami mengganti VMware Cloud Disaster Recovery dengan VMware Live Cyber Recovery dan mengganti VMware Site Recovery dengan VMware Live Site Recovery. Untuk informasi selengkapnya, lihat Catatan Rilis Pemulihan VMware Langsung.	September 4, 2024
VMware Akses HCX	Kami memperbarui AWS rekomendasi untuk mengonfig urasi VMware HCX untuk VMware Cloud aktif. AWS	Juni 5, 2023
Publikasi awal	—	November 3, 2022

AWS Glosarium Panduan Preskriptif

Berikut ini adalah istilah yang umum digunakan dalam strategi, panduan, dan pola yang disediakan oleh Panduan AWS Preskriptif. Untuk menyarankan entri, silakan gunakan tautan Berikan umpan balik di akhir glosarium.

Nomor

7 Rs

Tujuh strategi migrasi umum untuk memindahkan aplikasi ke cloud. Strategi ini dibangun di atas 5 Rs yang diidentifikasi Gartner pada tahun 2011 dan terdiri dari yang berikut:

- Refactor/Re-Architect — Memindahkan aplikasi dan memodifikasi arsitekturnya dengan memanfaatkan sepenuhnya fitur cloud-native untuk meningkatkan kelincahan, kinerja, dan skalabilitas. Ini biasanya melibatkan porting sistem operasi dan database. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Aurora PostgreSQL Compatible Edition.
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: Memigrasikan database Oracle lokal Anda ke Amazon Relational Database Service (Amazon RDS) untuk Oracle di. AWS Cloud
- Pembelian kembali (drop and shop) - Beralih ke produk yang berbeda, biasanya dengan beralih dari lisensi tradisional ke model SaaS. Contoh: Migrasikan sistem manajemen hubungan pelanggan (CRM) Anda ke Salesforce.com.
- Rehost (lift dan shift) — Pindahkan aplikasi ke cloud tanpa membuat perubahan apa pun untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Oracle pada instance EC2 di. AWS Cloud
- Relokasi (hypervisor-level lift and shift) — Pindahkan infrastruktur ke cloud tanpa membeli perangkat keras baru, menulis ulang aplikasi, atau memodifikasi operasi yang ada. Anda memigrasikan server dari platform lokal ke layanan cloud untuk platform yang sama. Contoh: Migrasikan Microsoft Hyper-V aplikasi ke AWS.
- Pertahankan (kunjungi kembali) - Simpan aplikasi di lingkungan sumber Anda. Ini mungkin termasuk aplikasi yang memerlukan refactoring besar, dan Anda ingin menunda pekerjaan itu sampai nanti, dan aplikasi lama yang ingin Anda pertahankan, karena tidak ada pembenaran bisnis untuk memigrasikannya.

- Pensiun — Menonaktifkan atau menghapus aplikasi yang tidak lagi diperlukan di lingkungan sumber Anda.

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

Metode migrasi database di mana database sumber dan target tetap sinkron (dengan menggunakan alat replikasi dua arah atau operasi penulisan ganda), dan kedua database menangani transaksi dari menghubungkan aplikasi selama migrasi. Metode ini mendukung migrasi dalam batch kecil yang terkontrol alih-alih memerlukan pemotongan satu kali. Ini lebih fleksibel tetapi membutuhkan lebih banyak pekerjaan daripada migrasi aktif-pasif.

migrasi aktif-pasif

Metode migrasi database di mana database sumber dan target disimpan dalam sinkron, tetapi hanya database sumber yang menangani transaksi dari menghubungkan aplikasi sementara data direplikasi ke database target. Basis data target tidak menerima transaksi apa pun selama migrasi.

fungsi agregat

Fungsi SQL yang beroperasi pada sekelompok baris dan menghitung nilai pengembalian tunggal untuk grup. Contoh fungsi agregat meliputi `SUM` dan`MAX`.

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

Proses menghapus informasi pribadi secara permanen dalam kumpulan data. Anonimisasi dapat membantu melindungi privasi pribadi. Data anonim tidak lagi dianggap sebagai data pribadi.

anti-pola

Solusi yang sering digunakan untuk masalah berulang di mana solusinya kontra-produktif, tidak efektif, atau kurang efektif daripada alternatif.

kontrol aplikasi

Pendekatan keamanan yang memungkinkan penggunaan hanya aplikasi yang disetujui untuk membantu melindungi sistem dari malware.

portofolio aplikasi

Kumpulan informasi rinci tentang setiap aplikasi yang digunakan oleh organisasi, termasuk biaya untuk membangun dan memelihara aplikasi, dan nilai bisnisnya. Informasi ini adalah kunci untuk penemuan portofolio dan proses analisis dan membantu mengidentifikasi dan memprioritaskan aplikasi yang akan dimigrasi, dimodernisasi, dan dioptimalkan.

kecerdasan buatan (AI)

Bidang ilmu komputer yang didedikasikan untuk menggunakan teknologi komputasi untuk melakukan fungsi kognitif yang biasanya terkait dengan manusia, seperti belajar, memecahkan masalah, dan mengenali pola. Untuk informasi lebih lanjut, lihat Apa itu Kecerdasan Buatan?

operasi kecerdasan buatan (AIOps)

Proses menggunakan teknik pembelajaran mesin untuk memecahkan masalah operasional, mengurangi insiden operasional dan intervensi manusia, dan meningkatkan kualitas layanan. Untuk informasi selengkapnya tentang cara AIOps digunakan dalam strategi AWS migrasi, lihat panduan integrasi operasi.

enkripsi asimetris

Algoritma enkripsi yang menggunakan sepasang kunci, kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi. Anda dapat berbagi kunci publik karena tidak digunakan untuk dekripsi, tetapi akses ke kunci pribadi harus sangat dibatasi.

atomisitas, konsistensi, isolasi, daya tahan (ACID)

Satu set properti perangkat lunak yang menjamin validitas data dan keandalan operasional database, bahkan dalam kasus kesalahan, kegagalan daya, atau masalah lainnya.

kontrol akses berbasis atribut (ABAC)

Praktik membuat izin berbutir halus berdasarkan atribut pengguna, seperti departemen, peran pekerjaan, dan nama tim. Untuk informasi selengkapnya, lihat ABAC untuk AWS dokumentasi AWS Identity and Access Management (IAM).

sumber data otoritatif

Lokasi di mana Anda menyimpan versi utama data, yang dianggap sebagai sumber informasi yang paling dapat diandalkan. Anda dapat menyalin data dari sumber data otoritatif ke lokasi lain untuk tujuan memproses atau memodifikasi data, seperti menganonimkan, menyunting, atau membuat nama samaran.

Zona Ketersediaan

Lokasi berbeda di dalam Wilayah AWS yang terisolasi dari kegagalan di Availability Zone lainnya dan menyediakan konektivitas jaringan latensi rendah yang murah ke Availability Zone lainnya di Wilayah yang sama.

AWS Kerangka Adopsi Cloud (AWS CAF)

Kerangka pedoman dan praktik terbaik AWS untuk membantu organisasi mengembangkan rencana yang efisien dan efektif untuk bergerak dengan sukses ke cloud. AWS CAF mengatur panduan ke dalam enam area fokus yang disebut perspektif: bisnis, orang, tata kelola, platform, keamanan, dan operasi. Perspektif bisnis, orang, dan tata kelola fokus pada keterampilan dan proses bisnis; perspektif platform, keamanan, dan operasi fokus pada keterampilan dan proses teknis. Misalnya, perspektif masyarakat menargetkan pemangku kepentingan yang menangani sumber daya manusia (SDM), fungsi kepegawaian, dan manajemen orang. Untuk perspektif ini, AWS CAF memberikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs web AWS CAF dan whitepaper AWS CAF.

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

Alat yang mengevaluasi beban kerja migrasi database, merekomendasikan strategi migrasi, dan memberikan perkiraan kerja. AWS WQF disertakan dengan AWS Schema Conversion Tool ()AWS SCT. Ini menganalisis skema database dan objek kode, kode aplikasi, dependensi, dan karakteristik kinerja, dan memberikan laporan penilaian.

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

Pandangan interaktif yang terpadu tentang perilaku dan interaksi sumber daya dari waktu ke waktu. Anda dapat menggunakan grafik perilaku dengan Amazon Detective untuk memeriksa upaya logon yang gagal, panggilan API yang mencurigakan, dan tindakan serupa. Untuk informasi selengkapnya, lihat Data dalam grafik perilaku di dokumentasi Detektif.

sistem big-endian

Sistem yang menyimpan byte paling signifikan terlebih dahulu. Lihat juga endianness.

klasifikasi biner

Sebuah proses yang memprediksi hasil biner (salah satu dari dua kelas yang mungkin). Misalnya, model ML Anda mungkin perlu memprediksi masalah seperti “Apakah email ini spam atau bukan spam?” atau “Apakah produk ini buku atau mobil?”

filter mekar

Struktur data probabilistik dan efisien memori yang digunakan untuk menguji apakah suatu elemen adalah anggota dari suatu himpunan.

deployment biru/hijau

Strategi penyebaran tempat Anda membuat dua lingkungan yang terpisah namun identik. Anda menjalankan versi aplikasi saat ini di satu lingkungan (biru) dan versi aplikasi baru di lingkungan lain (hijau). Strategi ini membantu Anda dengan cepat memutar kembali dengan dampak minimal.

bot

Aplikasi perangkat lunak yang menjalankan tugas otomatis melalui internet dan mensimulasikan aktivitas atau interaksi manusia. Beberapa bot berguna atau bermanfaat, seperti perayap web yang mengindeks informasi di internet. Beberapa bot lain, yang dikenal sebagai bot buruk, dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

botnet

Jaringan bot yang terinfeksi oleh malware dan berada di bawah kendali satu pihak, yang dikenal sebagai bot herder atau operator bot. Botnet adalah mekanisme paling terkenal untuk skala bot dan dampaknya.

cabang

Area berisi repositori kode. Cabang pertama yang dibuat dalam repositori adalah cabang utama. Anda dapat membuat cabang baru dari cabang yang ada, dan Anda kemudian dapat mengembangkan fitur atau memperbaiki bug di cabang baru. Cabang yang Anda buat untuk membangun fitur biasanya disebut sebagai cabang fitur. Saat fitur siap dirilis, Anda menggabungkan cabang fitur kembali ke cabang utama. Untuk informasi selengkapnya, lihat Tentang cabang (GitHub dokumentasi).

akses break-glass

Dalam keadaan luar biasa dan melalui proses yang disetujui, cara cepat bagi pengguna untuk mendapatkan akses ke Akun AWS yang biasanya tidak memiliki izin untuk mengaksesnya. Untuk informasi lebih lanjut, lihat indikator Implementasikan prosedur break-glass dalam panduan Well-Architected AWS .

strategi brownfield

Infrastruktur yang ada di lingkungan Anda. Saat mengadopsi strategi brownfield untuk arsitektur sistem, Anda merancang arsitektur di sekitar kendala sistem dan infrastruktur saat ini. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

Apa yang dilakukan bisnis untuk menghasilkan nilai (misalnya, penjualan, layanan pelanggan, atau pemasaran). Arsitektur layanan mikro dan keputusan pengembangan dapat didorong oleh kemampuan bisnis. Untuk informasi selengkapnya, lihat bagian Terorganisir di sekitar kemampuan bisnis dari Menjalankan layanan mikro kontainer di whitepaper. AWS

perencanaan kelangsungan bisnis (BCP)

Rencana yang membahas dampak potensial dari peristiwa yang mengganggu, seperti migrasi skala besar, pada operasi dan memungkinkan bisnis untuk melanjutkan operasi dengan cepat.

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

Rilis versi yang lambat dan bertahap untuk pengguna akhir. Ketika Anda yakin, Anda menyebarkan versi baru dan mengganti versi saat ini secara keseluruhan.

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

Proses melacak perubahan ke sumber data, seperti tabel database, dan merekam metadata tentang perubahan tersebut. Anda dapat menggunakan CDC untuk berbagai tujuan, seperti mengaudit atau mereplikasi perubahan dalam sistem target untuk mempertahankan sinkronisasi.

rekayasa kekacauan

Dengan sengaja memperkenalkan kegagalan atau peristiwa yang mengganggu untuk menguji ketahanan sistem. Anda dapat menggunakan AWS Fault Injection Service (AWS FIS) untuk melakukan eksperimen yang menekankan AWS beban kerja Anda dan mengevaluasi responsnya.

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

Proses kategorisasi yang membantu menghasilkan prediksi. Model ML untuk masalah klasifikasi memprediksi nilai diskrit. Nilai diskrit selalu berbeda satu sama lain. Misalnya, model mungkin perlu mengevaluasi apakah ada mobil dalam gambar atau tidak.

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat posting CCo E di Blog Strategi AWS Cloud Perusahaan.

komputasi cloud

Teknologi cloud yang biasanya digunakan untuk penyimpanan data jarak jauh dan manajemen perangkat IoT. Cloud computing umumnya terhubung ke teknologi edge computing.

model operasi cloud

Dalam organisasi TI, model operasi yang digunakan untuk membangun, mematangkan, dan mengoptimalkan satu atau lebih lingkungan cloud. Untuk informasi selengkapnya, lihat Membangun Model Operasi Cloud Anda.

tahap adopsi cloud

Empat fase yang biasanya dilalui organisasi ketika mereka bermigrasi ke AWS Cloud:

- Proyek — Menjalankan beberapa proyek terkait cloud untuk bukti konsep dan tujuan pembelajaran
- Foundation — Melakukan investasi dasar untuk meningkatkan adopsi cloud Anda (misalnya, membuat landing zone, mendefinisikan CCo E, membuat model operasi)
- Migrasi — Migrasi aplikasi individual
- Re-invention — Mengoptimalkan produk dan layanan, dan berinovasi di cloud

Tahapan ini didefinisikan oleh Stephen Orban dalam posting blog The Journey Toward Cloud-First & the Stages of Adoption di blog Strategi Perusahaan. AWS Cloud Untuk informasi tentang bagaimana kaitannya dengan strategi AWS migrasi, lihat panduan kesiapan migrasi.

CMDB

Lihat database manajemen konfigurasi.

repositori kode

Lokasi di mana kode sumber dan aset lainnya, seperti dokumentasi, sampel, dan skrip, disimpan dan diperbarui melalui proses kontrol versi. Repositori cloud umum termasuk GitHub atau. Bitbucket Cloud Setiap versi kode disebut cabang. Dalam struktur layanan mikro, setiap repositori

dikhususkan untuk satu bagian fungsionalitas. Pipa CI/CD tunggal dapat menggunakan beberapa repositori.

cache dingin

Cache buffer yang kosong, tidak terisi dengan baik, atau berisi data basi atau tidak relevan. Ini mempengaruhi kinerja karena instance database harus membaca dari memori utama atau disk, yang lebih lambat daripada membaca dari cache buffer.

data dingin

Data yang jarang diakses dan biasanya historis. Saat menanyakan jenis data ini, kueri lambat biasanya dapat diterima. Memindahkan data ini ke tingkat atau kelas penyimpanan yang berkinerja lebih rendah dan lebih murah dapat mengurangi biaya.

visi komputer (CV)

Bidang AI yang menggunakan pembelajaran mesin untuk menganalisis dan mengekstrak informasi dari format visual seperti gambar dan video digital. Misalnya, Amazon SageMaker AI menyediakan algoritma pemrosesan gambar untuk CV.

konfigurasi drift

Untuk beban kerja, konfigurasi berubah dari status yang diharapkan. Ini dapat menyebabkan beban kerja menjadi tidak patuh, dan biasanya bertahap dan tidak disengaja.

database manajemen konfigurasi (CMDB)

Repositori yang menyimpan dan mengelola informasi tentang database dan lingkungan TI, termasuk komponen perangkat keras dan perangkat lunak dan konfigurasinya. Anda biasanya menggunakan data dari CMDB dalam penemuan portofolio dan tahap analisis migrasi.

paket kesesuaian

Kumpulan AWS Config aturan dan tindakan remediasi yang dapat Anda kumpulkan untuk menyesuaikan kepatuhan dan pemeriksaan keamanan Anda. Anda dapat menerapkan paket kesesuaian sebagai entitas tunggal di Akun AWS dan Region, atau di seluruh organisasi, dengan menggunakan templat YAMM. Untuk informasi selengkapnya, lihat Paket kesesuaian dalam dokumentasi. AWS Config

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

Proses mengotomatiskan sumber, membangun, menguji, pementasan, dan tahap produksi dari proses rilis perangkat lunak. CI/CD is commonly described as a pipeline. CI/CDdapat membantu

Anda mengotomatiskan proses, meningkatkan produktivitas, meningkatkan kualitas kode, dan memberikan lebih cepat. Untuk informasi lebih lanjut, lihat Manfaat pengiriman berkelanjutan. CD juga dapat berarti penerapan berkelanjutan. Untuk informasi selengkapnya, lihat Continuous Delivery vs Continuous Deployment.

CV

Lihat visi komputer.

D

data saat istirahat

Data yang stasioner di jaringan Anda, seperti data yang ada di penyimpanan.

klasifikasi data

Proses untuk mengidentifikasi dan mengkategorikan data dalam jaringan Anda berdasarkan kekritisan dan sensitivitasnya. Ini adalah komponen penting dari setiap strategi manajemen risiko keamanan siber karena membantu Anda menentukan perlindungan dan kontrol retensi yang tepat untuk data. Klasifikasi data adalah komponen pilar keamanan dalam AWS Well-Architected Framework. Untuk informasi selengkapnya, lihat Klasifikasi data.

penyimpangan data

Variasi yang berarti antara data produksi dan data yang digunakan untuk melatih model ML, atau perubahan yang berarti dalam data input dari waktu ke waktu. Penyimpangan data dapat mengurangi kualitas, akurasi, dan keadilan keseluruhan dalam prediksi model ML.

data dalam transit

Data yang aktif bergerak melalui jaringan Anda, seperti antara sumber daya jaringan.

jala data

Kerangka arsitektur yang menyediakan kepemilikan data terdistribusi dan terdesentralisasi dengan manajemen dan tata kelola terpusat.

minimalisasi data

Prinsip pengumpulan dan pemrosesan hanya data yang sangat diperlukan. Mempraktikkan minimalisasi data di dalamnya AWS Cloud dapat mengurangi risiko privasi, biaya, dan jejak karbon analitik Anda.

perimeter data

Satu set pagar pembatas pencegahan di AWS lingkungan Anda yang membantu memastikan bahwa hanya identitas tepercaya yang mengakses sumber daya tepercaya dari jaringan yang diharapkan. Untuk informasi selengkapnya, lihat Membangun perimeter data pada AWS.

prapemrosesan data

Untuk mengubah data mentah menjadi format yang mudah diuraikan oleh model ML Anda. Preprocessing data dapat berarti menghapus kolom atau baris tertentu dan menangani nilai yang hilang, tidak konsisten, atau duplikat.

asal data

Proses melacak asal dan riwayat data sepanjang siklus hidupnya, seperti bagaimana data dihasilkan, ditransmisikan, dan disimpan.

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

Sistem manajemen data yang mendukung intelijen bisnis, seperti analitik. Gudang data biasanya berisi sejumlah besar data historis, dan biasanya digunakan untuk kueri dan analisis.

bahasa definisi database (DDL)

Pernyataan atau perintah untuk membuat atau memodifikasi struktur tabel dan objek dalam database.

bahasa manipulasi basis data (DHTML)

Pernyataan atau perintah untuk memodifikasi (memasukkan, memperbarui, dan menghapus) informasi dalam database.

DDL

Lihat bahasa definisi database.

ansambel yang dalam

Untuk menggabungkan beberapa model pembelajaran mendalam untuk prediksi. Anda dapat menggunakan ansambel dalam untuk mendapatkan prediksi yang lebih akurat atau untuk memperkirakan ketidakpastian dalam prediksi.

pembelajaran mendalam

Subbidang ML yang menggunakan beberapa lapisan jaringan saraf tiruan untuk mengidentifikasi pemetaan antara data input dan variabel target yang diinginkan.

defense-in-depth

Pendekatan keamanan informasi di mana serangkaian mekanisme dan kontrol keamanan dilapisi dengan cermat di seluruh jaringan komputer untuk melindungi kerahasiaan, integritas, dan ketersediaan jaringan dan data di dalamnya. Saat Anda mengadopsi strategi ini AWS, Anda menambahkan beberapa kontrol pada lapisan AWS Organizations struktur yang berbeda untuk membantu mengamankan sumber daya. Misalnya, defense-in-depth pendekatan mungkin menggabungkan otentikasi multi-faktor, segmentasi jaringan, dan enkripsi.

administrator yang didelegasikan

Di AWS Organizations, layanan yang kompatibel dapat mendaftarkan akun AWS anggota untuk mengelola akun organisasi dan mengelola izin untuk layanan tersebut. Akun ini disebut administrator yang didelegasikan untuk layanan itu. Untuk informasi selengkapnya dan daftar layanan yang kompatibel, lihat Layanan yang berfungsi dengan AWS Organizations AWS Organizations dokumentasi.

deployment

Proses pembuatan aplikasi, fitur baru, atau perbaikan kode tersedia di lingkungan target. Deployment melibatkan penerapan perubahan dalam basis kode dan kemudian membangun dan menjalankan basis kode itu di lingkungan aplikasi.

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

Kontrol keamanan yang dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan kedua, memperingatkan Anda tentang peristiwa keamanan yang melewati kontrol pencegahan di tempat. Untuk informasi selengkapnya, lihat Kontrol Detektif dalam Menerapkan kontrol keamanan pada. AWS

pemetaan aliran nilai pengembangan (DVSM)

Sebuah proses yang digunakan untuk mengidentifikasi dan memprioritaskan kendala yang mempengaruhi kecepatan dan kualitas dalam siklus hidup pengembangan perangkat lunak. DVSM memperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik

manufaktur ramping. Ini berfokus pada langkah-langkah dan tim yang diperlukan untuk menciptakan dan memindahkan nilai melalui proses pengembangan perangkat lunak.

kembar digital

Representasi virtual dari sistem dunia nyata, seperti bangunan, pabrik, peralatan industri, atau jalur produksi. Kembar digital mendukung pemeliharaan prediktif, pemantauan jarak jauh, dan optimalisasi produksi.

tabel dimensi

Dalam skema bintang, tabel yang lebih kecil yang berisi atribut data tentang data kuantitatif dalam tabel fakta. Atribut tabel dimensi biasanya bidang teks atau angka diskrit yang berperilaku seperti teks. Atribut ini biasanya digunakan untuk pembatasan kueri, pemfilteran, dan pelabelan set hasil.

musibah

Peristiwa yang mencegah beban kerja atau sistem memenuhi tujuan bisnisnya di lokasi utama yang digunakan. Peristiwa ini dapat berupa bencana alam, kegagalan teknis, atau akibat dari tindakan manusia, seperti kesalahan konfigurasi yang tidak disengaja atau serangan malware.

pemulihan bencana (DR)

Strategi dan proses yang Anda gunakan untuk meminimalkan downtime dan kehilangan data yang disebabkan oleh bencana. Untuk informasi selengkapnya, lihat Disaster Recovery of Workloads on AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

Pendekatan untuk mengembangkan sistem perangkat lunak yang kompleks dengan menghubungkan komponennya ke domain yang berkembang, atau tujuan bisnis inti, yang dilayani oleh setiap komponen. Konsep ini diperkenalkan oleh Eric Evans dalam bukunya, Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Untuk informasi tentang cara menggunakan desain berbasis domain dengan pola gambar pencekik, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

DR

Lihat pemulihan bencana.

deteksi drift

Melacak penyimpangan dari konfigurasi dasar. Misalnya, Anda dapat menggunakan AWS CloudFormation untuk mendeteksi penyimpangan dalam sumber daya sistem, atau Anda dapat menggunakannya AWS Control Tower untuk mendeteksi perubahan di landing zone yang mungkin memengaruhi kepatuhan terhadap persyaratan tata kelola.

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

Teknologi yang meningkatkan daya komputasi untuk perangkat pintar di tepi jaringan IoT. Jika dibandingkan dengan komputasi awan, komputasi tepi dapat mengurangi latensi komunikasi dan meningkatkan waktu respons.

pertukaran data elektronik (EDI)

Pertukaran otomatis dokumen bisnis antar organisasi. Untuk informasi selengkapnya, lihat Apa itu Pertukaran Data Elektronik.

enkripsi

Proses komputasi yang mengubah data plaintext, yang dapat dibaca manusia, menjadi ciphertext.

kunci enkripsi

String kriptografi dari bit acak yang dihasilkan oleh algoritma enkripsi. Panjang kunci dapat bervariasi, dan setiap kunci dirancang agar tidak dapat diprediksi dan unik.

endianness

Urutan byte disimpan dalam memori komputer. Sistem big-endian menyimpan byte paling signifikan terlebih dahulu. Sistem little-endian menyimpan byte paling tidak signifikan terlebih dahulu.

titik akhir

Lihat titik akhir layanan.

layanan endpoint

Layanan yang dapat Anda host di cloud pribadi virtual (VPC) untuk dibagikan dengan pengguna lain. Anda dapat membuat layanan endpoint dengan AWS PrivateLink dan memberikan izin kepada prinsipal lain Akun AWS atau ke AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (Amazon VPC).

perencanaan sumber daya perusahaan (ERP)

Sistem yang mengotomatiskan dan mengelola proses bisnis utama (seperti akuntansi, MES, dan manajemen proyek) untuk suatu perusahaan.

enkripsi amplop

Proses mengenkripsi kunci enkripsi dengan kunci enkripsi lain. Untuk informasi selengkapnya, lihat Enkripsi amplop dalam dokumentasi AWS Key Management Service (AWS KMS).

lingkungan

Sebuah contoh dari aplikasi yang sedang berjalan. Berikut ini adalah jenis lingkungan yang umum dalam komputasi awan:

- Development Environment — Sebuah contoh dari aplikasi yang berjalan yang hanya tersedia untuk tim inti yang bertanggung jawab untuk memelihara aplikasi. Lingkungan pengembangan digunakan untuk menguji perubahan sebelum mempromosikannya ke lingkungan atas. Jenis lingkungan ini kadang-kadang disebut sebagai lingkungan pengujian.
- lingkungan yang lebih rendah — Semua lingkungan pengembangan untuk aplikasi, seperti yang digunakan untuk build awal dan pengujian.
- lingkungan produksi — Sebuah contoh dari aplikasi yang berjalan yang pengguna akhir dapat mengakses. Dalam pipa CI/CD, lingkungan produksi adalah lingkungan penyebaran terakhir.
- lingkungan atas — Semua lingkungan yang dapat diakses oleh pengguna selain tim pengembangan inti. Ini dapat mencakup lingkungan produksi, lingkungan praproduksi, dan lingkungan untuk pengujian penerimaan pengguna.

epik

Dalam metodologi tangkas, kategori fungsional yang membantu mengatur dan memprioritaskan pekerjaan Anda. Epik memberikan deskripsi tingkat tinggi tentang persyaratan dan tugas implementasi. Misalnya, epos keamanan AWS CAF mencakup manajemen identitas dan akses, kontrol detektif, keamanan infrastruktur, perlindungan data, dan respons insiden. Untuk informasi selengkapnya tentang epos dalam strategi AWS migrasi, lihat panduan implementasi program.

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

Proses menganalisis dataset untuk memahami karakteristik utamanya. Anda mengumpulkan atau mengumpulkan data dan kemudian melakukan penyelidikan awal untuk menemukan pola, mendeteksi anomali, dan memeriksa asumsi. EDA dilakukan dengan menghitung statistik ringkasan dan membuat visualisasi data.

F

tabel fakta

Tabel tengah dalam skema bintang. Ini menyimpan data kuantitatif tentang operasi bisnis. Biasanya, tabel fakta berisi dua jenis kolom: kolom yang berisi ukuran dan yang berisi kunci asing ke tabel dimensi.

gagal cepat

Filosofi yang menggunakan pengujian yang sering dan bertahap untuk mengurangi siklus hidup pengembangan. Ini adalah bagian penting dari pendekatan tangkas.

batas isolasi kesalahan

Dalam AWS Cloud, batas seperti Availability Zone, Wilayah AWS, control plane, atau data plane yang membatasi efek kegagalan dan membantu meningkatkan ketahanan beban kerja. Untuk informasi selengkapnya, lihat Batas Isolasi AWS Kesalahan.

cabang fitur

Lihat cabang.

fitur

Data input yang Anda gunakan untuk membuat prediksi. Misalnya, dalam konteks manufaktur, fitur bisa berupa gambar yang diambil secara berkala dari lini manufaktur.

pentingnya fitur

Seberapa signifikan fitur untuk prediksi model. Ini biasanya dinyatakan sebagai skor numerik yang dapat dihitung melalui berbagai teknik, seperti Shapley Additive Explanations (SHAP) dan gradien terintegrasi. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

transformasi fitur

Untuk mengoptimalkan data untuk proses ML, termasuk memperkaya data dengan sumber tambahan, menskalakan nilai, atau mengekstrak beberapa set informasi dari satu bidang data. Hal ini memungkinkan model ML untuk mendapatkan keuntungan dari data. Misalnya, jika Anda memecah tanggal “2021-05-27 00:15:37" menjadi “2021", “Mei”, “Kamis”, dan “15", Anda dapat membantu algoritme pembelajaran mempelajari pola bernuansa yang terkait dengan komponen data yang berbeda.

beberapa tembakan mendorong

Menyediakan LLM dengan sejumlah kecil contoh yang menunjukkan tugas dan output yang diinginkan sebelum memintanya untuk melakukan tugas serupa. Teknik ini adalah aplikasi pembelajaran dalam konteks, di mana model belajar dari contoh (bidikan) yang tertanam dalam petunjuk. Beberapa bidikan dapat efektif untuk tugas-tugas yang memerlukan pemformatan, penalaran, atau pengetahuan domain tertentu. Lihat juga bidikan nol.

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

Metode migrasi database yang menggunakan replikasi data berkelanjutan melalui pengambilan data perubahan untuk memigrasikan data dalam waktu sesingkat mungkin, alih-alih menggunakan pendekatan bertahap. Tujuannya adalah untuk menjaga downtime seminimal mungkin.

FM

Lihat model pondasi.

model pondasi (FM)

Jaringan saraf pembelajaran mendalam yang besar yang telah melatih kumpulan data besar-besaran data umum dan tidak berlabel. FMs mampu melakukan berbagai tugas umum, seperti memahami bahasa, menghasilkan teks dan gambar, dan berbicara dalam bahasa alami. Untuk informasi selengkapnya, lihat Apa itu Model Foundation.

G

AI generatif

Subset model AI yang telah dilatih pada sejumlah besar data dan yang dapat menggunakan prompt teks sederhana untuk membuat konten dan artefak baru, seperti gambar, video, teks, dan audio. Untuk informasi lebih lanjut, lihat Apa itu AI Generatif.

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

Di Amazon CloudFront, opsi untuk mencegah pengguna di negara tertentu mengakses distribusi konten. Anda dapat menggunakan daftar izinkan atau daftar blokir untuk menentukan negara yang disetujui dan dilarang. Untuk informasi selengkapnya, lihat Membatasi distribusi geografis konten Anda dalam dokumentasi. CloudFront

Alur kerja Gitflow

Pendekatan di mana lingkungan bawah dan atas menggunakan cabang yang berbeda dalam repositori kode sumber. Alur kerja Gitflow dianggap warisan, dan alur kerja berbasis batang adalah pendekatan modern yang lebih disukai.

gambar emas

Sebuah snapshot dari sistem atau perangkat lunak yang digunakan sebagai template untuk menyebarkan instance baru dari sistem atau perangkat lunak itu. Misalnya, di bidang manufaktur, gambar emas dapat digunakan untuk menyediakan perangkat lunak pada beberapa perangkat dan membantu meningkatkan kecepatan, skalabilitas, dan produktivitas dalam operasi manufaktur perangkat.

strategi greenfield

Tidak adanya infrastruktur yang ada di lingkungan baru. Saat mengadopsi strategi greenfield untuk arsitektur sistem, Anda dapat memilih semua teknologi baru tanpa batasan kompatibilitas dengan infrastruktur yang ada, juga dikenal sebagai brownfield. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

pagar pembatas

Aturan tingkat tinggi yang membantu mengatur sumber daya, kebijakan, dan kepatuhan di seluruh unit organisasi ()OUs. Pagar pembatas preventif menegakkan kebijakan untuk memastikan keselarasan dengan standar kepatuhan. Mereka diimplementasikan dengan menggunakan kebijakan kontrol layanan dan batas izin IAM. Detective guardrails mendeteksi pelanggaran kebijakan dan masalah kepatuhan, dan menghasilkan peringatan untuk remediasi. Mereka diimplementasikan dengan menggunakan AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector, dan pemeriksaan khusus AWS Lambda .

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

Memigrasi database sumber Anda ke database target yang menggunakan mesin database yang berbeda (misalnya, Oracle ke Amazon Aurora). Migrasi heterogen biasanya merupakan bagian dari upaya arsitektur ulang, dan mengubah skema dapat menjadi tugas yang kompleks. AWS menyediakan AWS SCT yang membantu dengan konversi skema.

ketersediaan tinggi (HA)

Kemampuan beban kerja untuk beroperasi terus menerus, tanpa intervensi, jika terjadi tantangan atau bencana. Sistem HA dirancang untuk gagal secara otomatis, secara konsisten memberikan kinerja berkualitas tinggi, dan menangani beban dan kegagalan yang berbeda dengan dampak kinerja minimal.

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan

adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

data penahanan

Sebagian dari data historis berlabel yang ditahan dari kumpulan data yang digunakan untuk melatih model pembelajaran mesin. Anda dapat menggunakan data penahanan untuk mengevaluasi kinerja model dengan membandingkan prediksi model dengan data penahanan.

migrasi database homogen

Memigrasi database sumber Anda ke database target yang berbagi mesin database yang sama (misalnya, Microsoft SQL Server ke Amazon RDS for SQL Server). Migrasi homogen biasanya merupakan bagian dari upaya rehosting atau replatforming. Anda dapat menggunakan utilitas database asli untuk memigrasi skema.

data panas

Data yang sering diakses, seperti data real-time atau data translasi terbaru. Data ini biasanya memerlukan tingkat atau kelas penyimpanan berkinerja tinggi untuk memberikan respons kueri yang cepat.

perbaikan terbaru

Perbaikan mendesak untuk masalah kritis dalam lingkungan produksi. Karena urgensinya, perbaikan terbaru biasanya dibuat di luar alur kerja DevOps rilis biasa.

periode hypercare

Segera setelah cutover, periode waktu ketika tim migrasi mengelola dan memantau aplikasi yang dimigrasi di cloud untuk mengatasi masalah apa pun. Biasanya, periode ini panjangnya 1-4 hari. Pada akhir periode hypercare, tim migrasi biasanya mentransfer tanggung jawab untuk aplikasi ke tim operasi cloud.

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

Kebijakan yang dilampirkan pada satu atau beberapa prinsip IAM yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki penggunaan CPU dan memori rata-rata antara 5 dan 20 persen selama periode 90 hari. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini atau mempertahankannya di tempat.

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

Model yang menyebarkan infrastruktur baru untuk beban kerja produksi alih-alih memperbarui, menambal, atau memodifikasi infrastruktur yang ada. Infrastruktur yang tidak dapat diubah secara inheren lebih konsisten, andal, dan dapat diprediksi daripada infrastruktur yang dapat berubah. Untuk informasi selengkapnya, lihat praktik terbaik Deploy using immutable infrastructure di AWS Well-Architected Framework.

masuk (masuknya) VPC

Dalam arsitektur AWS multi-akun, VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

migrasi inkremental

Strategi cutover di mana Anda memigrasikan aplikasi Anda dalam bagian-bagian kecil alih-alih melakukan satu cutover penuh. Misalnya, Anda mungkin hanya memindahkan beberapa layanan mikro atau pengguna ke sistem baru pada awalnya. Setelah Anda memverifikasi bahwa semuanya berfungsi dengan baik, Anda dapat secara bertahap memindahkan layanan mikro atau pengguna tambahan hingga Anda dapat menonaktifkan sistem lama Anda. Strategi ini mengurangi risiko yang terkait dengan migrasi besar.

Industri 4.0

Sebuah istilah yang diperkenalkan oleh Klaus Schwab pada tahun 2016 untuk merujuk pada modernisasi proses manufaktur melalui kemajuan dalam konektivitas, data real-time, otomatisasi, analitik, dan AI/ML.

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

Proses penyediaan dan pengelolaan infrastruktur aplikasi melalui satu set file konfigurasi. IAc dirancang untuk membantu Anda memusatkan manajemen infrastruktur, menstandarisasi sumber daya, dan menskalakan dengan cepat sehingga lingkungan baru dapat diulang, andal, dan konsisten.

Internet of Things industri (IIoT)

Penggunaan sensor dan perangkat yang terhubung ke internet di sektor industri, seperti manufaktur, energi, otomotif, perawatan kesehatan, ilmu kehidupan, dan pertanian. Untuk informasi lebih lanjut, lihat Membangun strategi transformasi digital Internet of Things (IIoT) industri.

inspeksi VPC

Dalam arsitektur AWS multi-akun, VPC terpusat yang mengelola inspeksi lalu lintas jaringan antara VPCs (dalam yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

Internet of Things (IoT)

Jaringan objek fisik yang terhubung dengan sensor atau prosesor tertanam yang berkomunikasi dengan perangkat dan sistem lain melalui internet atau melalui jaringan komunikasi lokal. Untuk informasi selengkapnya, lihat Apa itu IoT?

interpretabilitas

Karakteristik model pembelajaran mesin yang menggambarkan sejauh mana manusia dapat memahami bagaimana prediksi model bergantung pada inputnya. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

Serangkaian praktik terbaik untuk memberikan layanan TI dan menyelaraskan layanan ini dengan persyaratan bisnis. ITIL menyediakan dasar untuk ITSM.

Manajemen layanan TI (ITSM)

Kegiatan yang terkait dengan merancang, menerapkan, mengelola, dan mendukung layanan TI untuk suatu organisasi. Untuk informasi tentang mengintegrasikan operasi cloud dengan alat ITSM, lihat panduan integrasi operasi.

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

Implementasi kontrol akses wajib (MAC) di mana pengguna dan data itu sendiri masing-masing secara eksplisit diberi nilai label keamanan. Persimpangan antara label keamanan pengguna dan label keamanan data menentukan baris dan kolom mana yang dapat dilihat oleh pengguna.

landing zone

Landing zone adalah AWS lingkungan multi-akun yang dirancang dengan baik yang dapat diskalakan dan aman. Ini adalah titik awal dari mana organisasi Anda dapat dengan cepat meluncurkan dan menyebarkan beban kerja dan aplikasi dengan percaya diri dalam lingkungan keamanan dan infrastruktur mereka. Untuk informasi selengkapnya tentang zona pendaratan, lihat Menyiapkan lingkungan multi-akun AWS yang aman dan dapat diskalakan.

model bahasa besar (LLM)

Model AI pembelajaran mendalam yang dilatih sebelumnya pada sejumlah besar data. LLM dapat melakukan beberapa tugas, seperti menjawab pertanyaan, meringkas dokumen, menerjemahkan teks ke dalam bahasa lain, dan menyelesaikan kalimat. Untuk informasi lebih lanjut, lihat Apa itu LLMs.

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

Praktik keamanan terbaik untuk memberikan izin minimum yang diperlukan untuk melakukan tugas. Untuk informasi selengkapnya, lihat Menerapkan izin hak istimewa terkecil dalam dokumentasi IAM.

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

Sebuah sistem yang menyimpan byte paling tidak signifikan terlebih dahulu. Lihat juga endianness.

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan pola dan pembelajaran. ML menganalisis dan belajar dari data yang direkam, seperti data Internet of Things (IoT), untuk menghasilkan model statistik berdasarkan pola. Untuk informasi selengkapnya, lihat Machine Learning.

cabang utama

Lihat cabang.

malware

Perangkat lunak yang dirancang untuk membahayakan keamanan atau privasi komputer. Malware dapat mengganggu sistem komputer, membocorkan informasi sensitif, atau mendapatkan akses yang tidak sah. Contoh malware termasuk virus, worm, ransomware, Trojan horse, spyware, dan keyloggers.

layanan terkelola

Layanan AWS yang AWS mengoperasikan lapisan infrastruktur, sistem operasi, dan platform, dan Anda mengakses titik akhir untuk menyimpan dan mengambil data. Amazon Simple Storage Service (Amazon S3) dan Amazon DynamoDB adalah contoh layanan terkelola. Ini juga dikenal sebagai layanan abstrak.

sistem eksekusi manufaktur (MES)

Sistem perangkat lunak untuk melacak, memantau, mendokumentasikan, dan mengendalikan proses produksi yang mengubah bahan baku menjadi produk jadi di lantai toko.

PETA

Lihat Program Percepatan Migrasi.

mekanisme

Proses lengkap di mana Anda membuat alat, mendorong adopsi alat, dan kemudian memeriksa hasilnya untuk melakukan penyesuaian. Mekanisme adalah siklus yang memperkuat dan meningkatkan dirinya sendiri saat beroperasi. Untuk informasi lebih lanjut, lihat Membangun mekanisme di AWS Well-Architected Framework.

akun anggota

Semua Akun AWS selain akun manajemen yang merupakan bagian dari organisasi di AWS Organizations. Akun dapat menjadi anggota dari hanya satu organisasi pada suatu waktu.

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

Protokol komunikasi ringan machine-to-machine (M2M), berdasarkan pola terbitkan/berlangganan, untuk perangkat IoT yang dibatasi sumber daya.

layanan mikro

Layanan kecil dan independen yang berkomunikasi dengan jelas APIs dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali, dan ketahanan. Untuk

informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

Pendekatan untuk membangun aplikasi dengan komponen independen yang menjalankan setiap proses aplikasi sebagai layanan mikro. Layanan mikro ini berkomunikasi melalui antarmuka yang terdefinisi dengan baik dengan menggunakan ringan. APIs Setiap layanan mikro dalam arsitektur ini dapat diperbarui, digunakan, dan diskalakan untuk memenuhi permintaan fungsi tertentu dari suatu aplikasi. Untuk informasi selengkapnya, lihat Menerapkan layanan mikro di AWS.

Program Percepatan Migrasi (MAP)

AWS Program yang menyediakan dukungan konsultasi, pelatihan, dan layanan untuk membantu organisasi membangun fondasi operasional yang kuat untuk pindah ke cloud, dan untuk membantu mengimbangi biaya awal migrasi. MAP mencakup metodologi migrasi untuk mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatisasi dan mempercepat skenario migrasi umum.

migrasi dalam skala

Proses memindahkan sebagian besar portofolio aplikasi ke cloud dalam gelombang, dengan lebih banyak aplikasi bergerak pada tingkat yang lebih cepat di setiap gelombang. Fase ini menggunakan praktik dan pelajaran terbaik dari fase sebelumnya untuk mengimplementasikan pabrik migrasi tim, alat, dan proses untuk merampingkan migrasi beban kerja melalui otomatisasi dan pengiriman tangkas. Ini adalah fase ketiga dari strategi AWS migrasi.

pabrik migrasi

Tim lintas fungsi yang merampingkan migrasi beban kerja melalui pendekatan otomatis dan gesit. Tim pabrik migrasi biasanya mencakup operasi, analis dan pemilik bisnis, insinyur migrasi, pengembang, dan DevOps profesional yang bekerja di sprint. Antara 20 dan 50 persen portofolio aplikasi perusahaan terdiri dari pola berulang yang dapat dioptimalkan dengan pendekatan pabrik. Untuk informasi selengkapnya, lihat diskusi tentang pabrik migrasi dan panduan Pabrik Migrasi Cloud di kumpulan konten ini.

metadata migrasi

Informasi tentang aplikasi dan server yang diperlukan untuk menyelesaikan migrasi. Setiap pola migrasi memerlukan satu set metadata migrasi yang berbeda. Contoh metadata migrasi termasuk subnet target, grup keamanan, dan akun. AWS

pola migrasi

Tugas migrasi berulang yang merinci strategi migrasi, tujuan migrasi, dan aplikasi atau layanan migrasi yang digunakan. Contoh: Rehost migrasi ke Amazon EC2 dengan Layanan Migrasi AWS Aplikasi.

Penilaian Portofolio Migrasi (MPA)

Alat online yang menyediakan informasi untuk memvalidasi kasus bisnis untuk bermigrasi ke. AWS Cloud MPA menyediakan penilaian portofolio terperinci (ukuran kanan server, harga, perbandingan TCO, analisis biaya migrasi) serta perencanaan migrasi (analisis data aplikasi dan pengumpulan data, pengelompokan aplikasi, prioritas migrasi, dan perencanaan gelombang). Alat MPA (memerlukan login) tersedia gratis untuk semua AWS konsultan dan konsultan APN Partner.

Penilaian Kesiapan Migrasi (MRA)

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana aksi untuk menutup kesenjangan yang diidentifikasi, menggunakan CAF. AWS Untuk informasi selengkapnya, lihat panduan kesiapan migrasi. MRA adalah tahap pertama dari strategi AWS migrasi.

strategi migrasi

Pendekatan yang digunakan untuk memigrasikan beban kerja ke file. AWS Cloud Untuk informasi lebih lanjut, lihat entri 7 Rs di glosarium ini dan lihat Memobilisasi organisasi Anda untuk mempercepat migrasi skala besar.

ML

Lihat pembelajaran mesin.

modernisasi

Mengubah aplikasi usang (warisan atau monolitik) dan infrastrukturnya menjadi sistem yang gesit, elastis, dan sangat tersedia di cloud untuk mengurangi biaya, mendapatkan efisiensi, dan memanfaatkan inovasi. Untuk informasi selengkapnya, lihat Strategi untuk memodernisasi aplikasi di. AWS Cloud

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta

jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi lebih lanjut, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di. AWS Cloud

aplikasi monolitik (monolit)

Aplikasi yang berjalan sebagai layanan tunggal dengan proses yang digabungkan secara ketat. Aplikasi monolitik memiliki beberapa kelemahan. Jika satu fitur aplikasi mengalami lonjakan permintaan, seluruh arsitektur harus diskalakan. Menambahkan atau meningkatkan fitur aplikasi monolitik juga menjadi lebih kompleks ketika basis kode tumbuh. Untuk mengatasi masalah ini, Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat Menguraikan monolit menjadi layanan mikro.

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

Sebuah proses yang membantu menghasilkan prediksi untuk beberapa kelas (memprediksi satu dari lebih dari dua hasil). Misalnya, model ML mungkin bertanya “Apakah produk ini buku, mobil, atau telepon?” atau “Kategori produk mana yang paling menarik bagi pelanggan ini?”

infrastruktur yang bisa berubah

Model yang memperbarui dan memodifikasi infrastruktur yang ada untuk beban kerja produksi. Untuk meningkatkan konsistensi, keandalan, dan prediktabilitas, AWS Well-Architected Framework merekomendasikan penggunaan infrastruktur yang tidak dapat diubah sebagai praktik terbaik.

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

Metode migrasi di mana beban kerja sumber diturunkan selama proses migrasi. Metode ini melibatkan waktu henti yang diperpanjang dan biasanya digunakan untuk beban kerja kecil dan tidak kritis.

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

Metode migrasi di mana beban kerja sumber disalin ke sistem target tanpa diambil offline. Aplikasi yang terhubung ke beban kerja dapat terus berfungsi selama migrasi. Metode ini melibatkan waktu henti nol hingga minimal dan biasanya digunakan untuk beban kerja produksi yang kritis.

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

Protokol komunikasi machine-to-machine (M2M) untuk otomasi industri. OPC-UA menyediakan standar interoperabilitas dengan enkripsi data, otentikasi, dan skema otorisasi.

perjanjian tingkat operasional (OLA)

Perjanjian yang menjelaskan apa yang dijanjikan kelompok TI fungsional untuk diberikan satu sama lain, untuk mendukung perjanjian tingkat layanan (SLA).

Tinjauan Kesiapan Operasional (ORR)

Daftar pertanyaan dan praktik terbaik terkait yang membantu Anda memahami, mengevaluasi, mencegah, atau mengurangi ruang lingkup insiden dan kemungkinan kegagalan. Untuk informasi lebih lanjut, lihat Ulasan Kesiapan Operasional (ORR) dalam Kerangka Kerja Well-Architected AWS .

teknologi operasional (OT)

Sistem perangkat keras dan perangkat lunak yang bekerja dengan lingkungan fisik untuk mengendalikan operasi industri, peralatan, dan infrastruktur. Di bidang manufaktur, integrasi sistem OT dan teknologi informasi (TI) adalah fokus utama untuk transformasi Industri 4.0.

integrasi operasi (OI)

Proses modernisasi operasi di cloud, yang melibatkan perencanaan kesiapan, otomatisasi, dan integrasi. Untuk informasi selengkapnya, lihat panduan integrasi operasi.

jejak organisasi

Jejak yang dibuat oleh AWS CloudTrail itu mencatat semua peristiwa untuk semua Akun AWS dalam organisasi di AWS Organizations. Jejak ini dibuat di setiap Akun AWS bagian organisasi dan melacak aktivitas di setiap akun. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dalam CloudTrail dokumentasi.

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. OCM membantu organisasi mempersiapkan, dan transisi ke, sistem dan strategi baru dengan mempercepat adopsi perubahan, mengatasi masalah transisi, dan mendorong perubahan budaya dan organisasi. Dalam strategi AWS migrasi, kerangka kerja ini disebut percepatan orang, karena kecepatan perubahan yang diperlukan dalam proyek adopsi cloud. Untuk informasi lebih lanjut, lihat panduan OCM.

kontrol akses asal (OAC)

Di CloudFront, opsi yang disempurnakan untuk membatasi akses untuk mengamankan konten Amazon Simple Storage Service (Amazon S3) Anda. OAC mendukung semua bucket S3 di semua Wilayah AWS, enkripsi sisi server dengan AWS KMS (SSE-KMS), dan dinamis dan permintaan ke bucket S3. `PUT` `DELETE`

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakan OAI, CloudFront buat prinsipal yang dapat diautentikasi oleh Amazon S3. Prinsipal yang diautentikasi dapat mengakses konten dalam bucket S3 hanya melalui distribusi tertentu. CloudFront Lihat juga OAC, yang menyediakan kontrol akses yang lebih terperinci dan ditingkatkan.

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

Dalam arsitektur AWS multi-akun, VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

Kebijakan manajemen IAM yang dilampirkan pada prinsipal IAM untuk menetapkan izin maksimum yang dapat dimiliki pengguna atau peran. Untuk informasi selengkapnya, lihat Batas izin dalam dokumentasi IAM.

Informasi Identifikasi Pribadi (PII)

Informasi yang, jika dilihat secara langsung atau dipasangkan dengan data terkait lainnya, dapat digunakan untuk menyimpulkan identitas individu secara wajar. Contoh PII termasuk nama, alamat, dan informasi kontak.

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

Serangkaian langkah yang telah ditentukan sebelumnya yang menangkap pekerjaan yang terkait dengan migrasi, seperti mengirimkan fungsi operasi inti di cloud. Buku pedoman dapat berupa skrip, runbook otomatis, atau ringkasan proses atau langkah-langkah yang diperlukan untuk mengoperasikan lingkungan modern Anda.

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

Objek yang dapat menentukan izin (lihat kebijakan berbasis identitas), menentukan kondisi akses (lihat kebijakan berbasis sumber daya), atau menentukan izin maksimum untuk semua akun di organisasi (lihat kebijakan kontrol layanan). AWS Organizations

ketekunan poliglot

Secara independen memilih teknologi penyimpanan data microservice berdasarkan pola akses data dan persyaratan lainnya. Jika layanan mikro Anda memiliki teknologi penyimpanan data yang sama, mereka dapat menghadapi tantangan implementasi atau mengalami kinerja yang buruk. Layanan mikro lebih mudah diimplementasikan dan mencapai kinerja dan skalabilitas yang lebih baik jika mereka menggunakan penyimpanan data yang paling sesuai dengan kebutuhan mereka. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi data di layanan mikro.

penilaian portofolio

Proses menemukan, menganalisis, dan memprioritaskan portofolio aplikasi untuk merencanakan migrasi. Untuk informasi selengkapnya, lihat Mengevaluasi kesiapan migrasi.

predikat

Kondisi kueri yang mengembalikan `true` atau`false`, biasanya terletak di `WHERE` klausa.

predikat pushdown

Teknik optimasi kueri database yang menyaring data dalam kueri sebelum transfer. Ini mengurangi jumlah data yang harus diambil dan diproses dari database relasional, dan meningkatkan kinerja kueri.

kontrol preventif

Kontrol keamanan yang dirancang untuk mencegah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan pertama untuk membantu mencegah akses tidak sah atau perubahan yang tidak diinginkan ke jaringan Anda. Untuk informasi selengkapnya, lihat Kontrol pencegahan dalam Menerapkan kontrol keamanan pada. AWS

principal

Entitas AWS yang dapat melakukan tindakan dan mengakses sumber daya. Entitas ini biasanya merupakan pengguna root untuk Akun AWS, peran IAM, atau pengguna. Untuk informasi selengkapnya, lihat Prinsip dalam istilah dan konsep Peran dalam dokumentasi IAM.

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona yang dihosting pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau lebih. VPCs Untuk informasi selengkapnya, lihat Bekerja dengan zona yang dihosting pribadi di dokumentasi Route 53.

kontrol proaktif

Kontrol keamanan yang dirancang untuk mencegah penyebaran sumber daya yang tidak sesuai. Kontrol ini memindai sumber daya sebelum disediakan. Jika sumber daya tidak sesuai dengan kontrol, maka itu tidak disediakan. Untuk informasi selengkapnya, lihat panduan referensi Kontrol dalam AWS Control Tower dokumentasi dan lihat Kontrol proaktif dalam Menerapkan kontrol keamanan pada AWS.

manajemen siklus hidup produk (PLM)

Manajemen data dan proses untuk suatu produk di seluruh siklus hidupnya, mulai dari desain, pengembangan, dan peluncuran, melalui pertumbuhan dan kematangan, hingga penurunan dan penghapusan.

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

Di bidang manufaktur, komputer yang sangat andal dan mudah beradaptasi yang memantau mesin dan mengotomatiskan proses manufaktur.

rantai cepat

Menggunakan output dari satu prompt LLM sebagai input untuk prompt berikutnya untuk menghasilkan respons yang lebih baik. Teknik ini digunakan untuk memecah tugas yang kompleks menjadi subtugas, atau untuk secara iteratif memperbaiki atau memperluas respons awal. Ini membantu meningkatkan akurasi dan relevansi respons model dan memungkinkan hasil yang lebih terperinci dan dipersonalisasi.

pseudonimisasi

Proses penggantian pengenal pribadi dalam kumpulan data dengan nilai placeholder. Pseudonimisasi dapat membantu melindungi privasi pribadi. Data pseudonim masih dianggap sebagai data pribadi.

publish/subscribe (pub/sub)

Pola yang memungkinkan komunikasi asinkron antara layanan mikro untuk meningkatkan skalabilitas dan daya tanggap. Misalnya, dalam MES berbasis layanan mikro, layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan layanan mikro lainnya. Sistem dapat menambahkan layanan mikro baru tanpa mengubah layanan penerbitan.

Q

rencana kueri

Serangkaian langkah, seperti instruksi, yang digunakan untuk mengakses data dalam sistem database relasional SQL.

regresi rencana kueri

Ketika pengoptimal layanan database memilih rencana yang kurang optimal daripada sebelum perubahan yang diberikan ke lingkungan database. Hal ini dapat disebabkan oleh perubahan statistik, kendala, pengaturan lingkungan, pengikatan parameter kueri, dan pembaruan ke mesin database.

R

Matriks RACI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

LAP

Lihat Retrieval Augmented Generation.

ransomware

Perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data sampai pembayaran dilakukan.

Matriks RASCI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

Salinan database yang digunakan untuk tujuan read-only. Anda dapat merutekan kueri ke replika baca untuk mengurangi beban pada database utama Anda.

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

Jumlah waktu maksimum yang dapat diterima sejak titik pemulihan data terakhir. Ini menentukan apa yang dianggap sebagai kehilangan data yang dapat diterima antara titik pemulihan terakhir dan gangguan layanan.

tujuan waktu pemulihan (RTO)

Penundaan maksimum yang dapat diterima antara gangguan layanan dan pemulihan layanan.

refactor

Lihat 7 Rs.

Wilayah

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing Wilayah AWS terisolasi dan independen dari yang lain untuk memberikan toleransi kesalahan, stabilitas, dan ketahanan. Untuk informasi selengkapnya, lihat Menentukan Wilayah AWS akun yang dapat digunakan.

regresi

Teknik ML yang memprediksi nilai numerik. Misalnya, untuk memecahkan masalah “Berapa harga rumah ini akan dijual?” Model ML dapat menggunakan model regresi linier untuk memprediksi harga jual rumah berdasarkan fakta yang diketahui tentang rumah (misalnya, luas persegi).

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

Kemampuan aplikasi untuk melawan atau pulih dari gangguan. Ketersediaan tinggi dan pemulihan bencana adalah pertimbangan umum ketika merencanakan ketahanan di. AWS Cloud Untuk informasi lebih lanjut, lihat AWS Cloud Ketahanan.

kebijakan berbasis sumber daya

Kebijakan yang dilampirkan ke sumber daya, seperti bucket Amazon S3, titik akhir, atau kunci enkripsi. Jenis kebijakan ini menentukan prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

matriks yang bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI)

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Tipe dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut matriks RASCI, dan jika Anda mengecualikannya, itu disebut matriks RACI.

kontrol responsif

Kontrol keamanan yang dirancang untuk mendorong remediasi efek samping atau penyimpangan dari garis dasar keamanan Anda. Untuk informasi selengkapnya, lihat Kontrol responsif dalam Menerapkan kontrol keamanan pada AWS.

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

Teknologi AI generatif di mana LLM merujuk sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, model RAG mungkin melakukan pencarian semantik dari basis pengetahuan organisasi atau data kustom. Untuk informasi lebih lanjut, lihat Apa itu RAG.

rotasi

Proses memperbarui rahasia secara berkala untuk membuatnya lebih sulit bagi penyerang untuk mengakses kredensil.

kontrol akses baris dan kolom (RCAC)

Penggunaan ekspresi SQL dasar dan fleksibel yang telah menetapkan aturan akses. RCAC terdiri dari izin baris dan topeng kolom.

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

Satu set prosedur manual atau otomatis yang diperlukan untuk melakukan tugas tertentu. Ini biasanya dibangun untuk merampingkan operasi berulang atau prosedur dengan tingkat kesalahan yang tinggi.

D

SAML 2.0

Standar terbuka yang digunakan oleh banyak penyedia identitas (IdPs). Fitur ini memungkinkan sistem masuk tunggal gabungan (SSO), sehingga pengguna dapat masuk ke AWS Management Console atau memanggil operasi AWS API tanpa Anda harus membuat pengguna di IAM untuk semua orang di organisasi Anda. Untuk informasi lebih lanjut tentang federasi berbasis SAMP 2.0, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

Dalam AWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensi pengguna, yang Anda simpan dalam bentuk terenkripsi. Ini terdiri dari nilai rahasia dan metadata-nya. Nilai rahasia dapat berupa biner, string tunggal, atau beberapa string. Untuk informasi selengkapnya, lihat Apa yang ada di rahasia Secrets Manager? dalam dokumentasi Secrets Manager.

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

Pagar pembatas teknis atau administratif yang mencegah, mendeteksi, atau mengurangi kemampuan pelaku ancaman untuk mengeksploitasi kerentanan keamanan. Ada empat jenis kontrol keamanan utama: preventif, detektif, responsif, dan proaktif.

pengerasan keamanan

Proses mengurangi permukaan serangan untuk membuatnya lebih tahan terhadap serangan. Ini dapat mencakup tindakan seperti menghapus sumber daya yang tidak lagi diperlukan, menerapkan praktik keamanan terbaik untuk memberikan hak istimewa paling sedikit, atau menonaktifkan fitur yang tidak perlu dalam file konfigurasi.

sistem informasi keamanan dan manajemen acara (SIEM)

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen acara keamanan (SEM). Sistem SIEM mengumpulkan, memantau, dan menganalisis data dari server, jaringan, perangkat, dan sumber lain untuk mendeteksi ancaman dan pelanggaran keamanan, dan untuk menghasilkan peringatan.

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan

detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup keamanan VPC, menambal instans EC2 Amazon, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCPs menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCPs daftar izin atau daftar penolakan, untuk menentukan layanan atau tindakan mana yang diizinkan atau dilarang. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam AWS Organizations dokumentasi.

titik akhir layanan

URL titik masuk untuk file Layanan AWS. Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat Layanan AWS titik akhir di Referensi Umum AWS.

perjanjian tingkat layanan (SLA)

Perjanjian yang menjelaskan apa yang dijanjikan tim TI untuk diberikan kepada pelanggan mereka, seperti waktu kerja dan kinerja layanan.

indikator tingkat layanan (SLI)

Pengukuran aspek kinerja layanan, seperti tingkat kesalahan, ketersediaan, atau throughputnya.

tujuan tingkat layanan (SLO)

Metrik target yang mewakili kesehatan layanan, yang diukur dengan indikator tingkat layanan.

model tanggung jawab bersama

Model yang menjelaskan tanggung jawab yang Anda bagikan AWS untuk keamanan dan kepatuhan cloud. AWS bertanggung jawab atas keamanan cloud, sedangkan Anda bertanggung jawab atas keamanan di cloud. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

Kegagalan dalam satu komponen penting dari aplikasi yang dapat mengganggu sistem.

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

Struktur organisasi database yang menggunakan satu tabel fakta besar untuk menyimpan data transaksional atau terukur dan menggunakan satu atau lebih tabel dimensi yang lebih kecil untuk menyimpan atribut data. Struktur ini dirancang untuk digunakan dalam gudang data atau untuk tujuan intelijen bisnis.

pola ara pencekik

Pendekatan untuk memodernisasi sistem monolitik dengan menulis ulang secara bertahap dan mengganti fungsionalitas sistem sampai sistem warisan dapat dinonaktifkan. Pola ini menggunakan analogi pohon ara yang tumbuh menjadi pohon yang sudah mapan dan akhirnya mengatasi dan menggantikan inangnya. Pola ini diperkenalkan oleh Martin Fowler sebagai cara untuk mengelola risiko saat menulis ulang sistem monolitik. Untuk contoh cara menerapkan pola ini, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

subnet

Rentang alamat IP dalam VPC Anda. Subnet harus berada di Availability Zone tunggal.

kontrol pengawasan dan akuisisi data (SCADA)

Di bidang manufaktur, sistem yang menggunakan perangkat keras dan perangkat lunak untuk memantau aset fisik dan operasi produksi.

enkripsi simetris

Algoritma enkripsi yang menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.

pengujian sintetis

Menguji sistem dengan cara yang mensimulasikan interaksi pengguna untuk mendeteksi potensi masalah atau untuk memantau kinerja. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat tes ini.

sistem prompt

Teknik untuk memberikan konteks, instruksi, atau pedoman ke LLM untuk mengarahkan perilakunya. Permintaan sistem membantu mengatur konteks dan menetapkan aturan untuk interaksi dengan pengguna.

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Tanda dapat membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda.

variabel target

Nilai yang Anda coba prediksi dalam ML yang diawasi. Ini juga disebut sebagai variabel hasil. Misalnya, dalam pengaturan manufaktur, variabel target bisa menjadi cacat produk.

daftar tugas

Alat yang digunakan untuk melacak kemajuan melalui runbook. Daftar tugas berisi ikhtisar runbook dan daftar tugas umum yang harus diselesaikan. Untuk setiap tugas umum, itu termasuk perkiraan jumlah waktu yang dibutuhkan, pemilik, dan kemajuan.

lingkungan uji

Lihat lingkungan.

pelatihan

Untuk menyediakan data bagi model ML Anda untuk dipelajari. Data pelatihan harus berisi jawaban yang benar. Algoritma pembelajaran menemukan pola dalam data pelatihan yang memetakan atribut data input ke target (jawaban yang ingin Anda prediksi). Ini menghasilkan model ML yang menangkap pola-pola ini. Anda kemudian dapat menggunakan model ML untuk membuat prediksi pada data baru yang Anda tidak tahu targetnya.

gerbang transit

Hub transit jaringan yang dapat Anda gunakan untuk menghubungkan jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

Pendekatan di mana pengembang membangun dan menguji fitur secara lokal di cabang fitur dan kemudian menggabungkan perubahan tersebut ke cabang utama. Cabang utama kemudian dibangun untuk pengembangan, praproduksi, dan lingkungan produksi, secara berurutan.

akses tepercaya

Memberikan izin ke layanan yang Anda tentukan untuk melakukan tugas di organisasi Anda di dalam AWS Organizations dan di akunnya atas nama Anda. Layanan tepercaya menciptakan peran terkait layanan di setiap akun, ketika peran itu diperlukan, untuk melakukan tugas manajemen untuk Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan AWS layanan lain dalam AWS Organizations dokumentasi.

penyetelan

Untuk mengubah aspek proses pelatihan Anda untuk meningkatkan akurasi model ML. Misalnya, Anda dapat melatih model ML dengan membuat set pelabelan, menambahkan label, dan kemudian mengulangi langkah-langkah ini beberapa kali di bawah pengaturan yang berbeda untuk mengoptimalkan model.

tim dua pizza

Sebuah DevOps tim kecil yang bisa Anda beri makan dengan dua pizza. Ukuran tim dua pizza memastikan peluang terbaik untuk berkolaborasi dalam pengembangan perangkat lunak.

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian: ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data. Untuk informasi lebih lanjut, lihat panduan Mengukur ketidakpastian dalam sistem pembelajaran mendalam.

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

Operasi pemeliharaan database yang melibatkan pembersihan setelah pembaruan tambahan untuk merebut kembali penyimpanan dan meningkatkan kinerja.

kendali versi

Proses dan alat yang melacak perubahan, seperti perubahan kode sumber dalam repositori.

Peering VPC

Koneksi antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas dengan menggunakan alamat IP pribadi. Untuk informasi selengkapnya, lihat Apa itu peering VPC di dokumentasi VPC Amazon.

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data saat ini dan relevan yang sering diakses. Instance database dapat membaca dari cache buffer, yang lebih cepat daripada membaca dari memori utama atau disk.

data hangat

Data yang jarang diakses. Saat menanyakan jenis data ini, kueri yang cukup lambat biasanya dapat diterima.

fungsi jendela

Fungsi SQL yang melakukan perhitungan pada sekelompok baris yang berhubungan dengan catatan saat ini. Fungsi jendela berguna untuk memproses tugas, seperti menghitung rata-rata bergerak atau mengakses nilai baris berdasarkan posisi relatif dari baris saat ini.

beban kerja

Kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti aplikasi yang dihadapi pelanggan atau proses backend.

aliran kerja

Grup fungsional dalam proyek migrasi yang bertanggung jawab atas serangkaian tugas tertentu. Setiap alur kerja independen tetapi mendukung alur kerja lain dalam proyek. Misalnya, alur kerja portofolio bertanggung jawab untuk memprioritaskan aplikasi, perencanaan gelombang, dan mengumpulkan metadata migrasi. Alur kerja portofolio mengirimkan aset ini ke alur kerja migrasi, yang kemudian memigrasikan server dan aplikasi.

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

Model penyimpanan yang menulis data satu kali dan mencegah data dihapus atau dimodifikasi. Pengguna yang berwenang dapat membaca data sebanyak yang diperlukan, tetapi mereka tidak dapat mengubahnya. Infrastruktur penyimpanan data ini dianggap tidak dapat diubah.

Z

eksploitasi zero-day

Serangan, biasanya malware, yang memanfaatkan kerentanan zero-day.

kerentanan zero-day

Cacat atau kerentanan yang tak tanggung-tanggung dalam sistem produksi. Aktor ancaman dapat menggunakan jenis kerentanan ini untuk menyerang sistem. Pengembang sering menyadari kerentanan sebagai akibat dari serangan tersebut.

bisikan zero-shot

Memberikan LLM dengan instruksi untuk melakukan tugas tetapi tidak ada contoh (tembakan) yang dapat membantu membimbingnya. LLM harus menggunakan pengetahuan pra-terlatih untuk menangani tugas. Efektivitas bidikan nol tergantung pada kompleksitas tugas dan kualitas prompt. Lihat juga beberapa bidikan yang diminta.

aplikasi zombie

Aplikasi yang memiliki CPU rata-rata dan penggunaan memori di bawah 5 persen. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.