Pendekatan Backup dan Recovery pada AWS

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Pendekatan Backup dan Recovery pada AWS

Table of Contents

Pengantar 1
Mengapa digunakan AWS sebagai platform perlindungan data? 2
Hasil bisnis yang ditargetkan 4
Memilih AWS layanan 5
Merancang solusi cadangan dan pemulihan 8
AWS Backup 9
Amazon S3 11
Menggunakan kelas penyimpanan Amazon S3 11
Membuat ember S3 standar 13
Menggunakan versi Amazon S3 13
Mencadangkan dan memulihkan file konfigurasi khusus untuk AMI 13
Pencadangan dan pemulihan khusus 14
Mengamankan data cadangan 14
Amazon EC2 dengan volume EBS 15
Pencadangan dan pemulihan Amazon EC2 17
AMI atau snapshot 17
Volume server 19
Volume server terpisah 20
Volume penyimpanan instans 20
Menandai dan menegakkan standar 21
Buat cadangan volume EBS 22
Mempersiapkan volume EBS 22
Membuat snapshot dari konsol 24
Membuat AMI 24
Amazon Data Lifecycle Manager 25
AWS Backup 26
Pencadangan multi-volume 26
Melindungi cadangan 28
Mengarsipkan snapshot 29
Mengotomatiskan snapshot dan pembuatan AMI 29
Kembalikan volume atau instance 30
Memulihkan file dan direktori dari snapshot EBS 31
Memulihkan volume EBS dari snapshot Amazon EBS 31
Membuat atau memulihkan instans EC2 dari snapshot EBS 33

Memulihkan instance yang sedang berjalan dari AMI 34
Backup dan pemulihan dari lokal 35
Gerbang file 36
Gerbang volume 36
Gerbang pita 37
Backup dan pemulihan aplikasi 39
AWSLayanan cloud-native 40
Amazon RDS 40
Menggunakan CNAME 41
DynamoDB 43
Arsitektur hibrida 45
Memindahkan solusi manajemen cadangan terpusat 46
Pemulihan bencana 48
DR di tempat ke AWS 48
DR untuk beban kerja cloud-native 50
DR dalam satu Availability Zone 51
DR dalam kegagalan regional 51
Membersihkan backup 53
Pertanyaan yang Sering Diajukan 54
Jadwal cadangan apa yang harus saya pilih? 54
Apakah saya perlu membuat cadangan di akun pengembangan saya? 54
Dapatkah saya meningkatkan aplikasi dan terus menggunakan volume EBS saat snapshot dibuat tanpa dampak apa pun? 54
Langkah selanjutnya 55
Sumber daya 56
Riwayat dokumen 58
Glosarium 61
..... 61
A 62
B 65
C 67
D 70
E 74
F 76
G 77
H 78

I 79
L 82
M 83
O 87
P 89
Q 92
R 93
D 95
T 99
U 101
V 101
W 102
Z 103
..... civ

Pendekatan Backup dan Recovery pada AWS

Khurram Nizami, Amazon Web Services ()AWS

Juni 2024 (sejarah dokumen)

Panduan ini membahas cara menerapkan pendekatan pencadangan dan pemulihan menggunakan layanan Amazon Web Services (AWS) untuk arsitektur lokal, cloud-native, dan hybrid. Pendekatan ini menawarkan biaya yang lebih rendah, skalabilitas yang lebih tinggi, dan daya tahan yang lebih untuk memenuhi tujuan waktu pemulihan (RTO), tujuan titik pemulihan (RPO), dan persyaratan kepatuhan.

Panduan ini ditujukan untuk para pemimpin teknis yang bertanggung jawab untuk melindungi data di lingkungan TI dan cloud perusahaan mereka.

Panduan ini mencakup arsitektur cadangan yang berbeda (aplikasi cloud-native, hybrid, dan lingkungan lokal). Ini juga mencakup layanan Amazon Web Services (AWS) terkait yang dapat digunakan untuk membangun solusi perlindungan data yang dapat diskalakan dan andal untuk komponen arsitektur Anda yang tidak dapat diubah.

Pendekatan lain adalah memodernisasi beban kerja Anda untuk menggunakan arsitektur yang tidak dapat diubah, mengurangi kebutuhan untuk pencadangan dan pemulihan komponen. AWS menyediakan sejumlah layanan untuk mengimplementasikan arsitektur yang tidak dapat diubah dan mengurangi kebutuhan untuk pencadangan dan pemulihan, termasuk:

- Tanpa server dengan AWS Lambda
- Wadah dengan Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), dan AWS Fargate
- Gambar Mesin Amazon (AMI) dengan Amazon Elastic Compute Cloud (Amazon EC2)

Seiring dengan percepatan pertumbuhan data perusahaan, tugas melindunginya menjadi lebih menantang. Pertanyaan tentang daya tahan dan skalabilitas pendekatan pencadangan adalah hal biasa, termasuk yang ini: Bagaimana cloud membantu memenuhi kebutuhan pencadangan dan pemulihan saya?

Panduan ini mencakup topik-topik berikut:

- Memilih AWS layanan untuk perlindungan data
- Merancang solusi cadangan dan pemulihan

- Backup dan pemulihan menggunakanAWS Backup
- Backup dan pemulihan menggunakan Amazon S3
- Backup dan pemulihan untuk Amazon EC2 dengan volume EBS
- Backup dan pemulihan dari infrastruktur lokal ke AWS
- Backup dan pemulihan aplikasi dariAWSke pusat data Anda
- Backup dan pemulihanAWS layanan cloud-native
- Backup dan recovery untuk arsitektur hybrid
- Pemulihan bencana dengan AWS
- Membersihkan backup

Mengapa digunakan AWS sebagai platform perlindungan data?

AWS adalah platform komputasi awan yang aman, berkinerja tinggi, fleksibel, hemat uang, dan easy-to-use komputasi awan. AWS menangani pengangkatan berat yang tidak berdiferensiasi yang diperlukan untuk membuat, mengimplementasikan, dan mengelola solusi pencadangan dan pemulihan yang dapat diskalakan.

Ada banyak keuntungan untuk digunakan AWS sebagai bagian dari strategi perlindungan data Anda:

- Daya tahan: Amazon Simple Storage Service (Amazon S3) dan S3 Glacier Deep Archive dirancang untuk daya tahan 99,999999999 persen (11 sembilan). Kedua platform menawarkan cadangan data yang andal, dengan replikasi objek di setidaknya tiga Availability Zone yang tersebar secara geografis. Banyak AWS layanan menggunakan Amazon S3 untuk operasi penyimpanan dan ekspor/impor. Misalnya, Amazon Elastic Block Store (Amazon EBS) menggunakan Amazon S3 untuk penyimpanan snapshot.
- Keamanan: AWS menyediakan sejumlah opsi untuk kontrol akses dan enkripsi data saat dalam perjalanan dan istirahat.
- Infrastruktur global: AWS layanan tersedia di seluruh dunia, sehingga Anda dapat mencadangkan dan menyimpan data di Wilayah yang memenuhi persyaratan kepatuhan dan beban kerja Anda.
- Kepatuhan: AWS infrastruktur disertifikasi untuk memenuhi standar berikut, sehingga Anda dapat dengan mudah memasukkan solusi cadangan ke dalam rejimen kepatuhan yang ada:
  - Kontrol Organisasi Layanan (SOC)
  - Pernyataan tentang Standar untuk Keterlibatan Pengesahan (SSAE) 16
  - Organisasi Internasional untuk Standardisasi (ISO) 27001

  - Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)
  - Undang-Undang Akuntabilitas dan Portabilitas Asuransi Kesehatan (HIPAA)
  - SEC1
  - Program Manajemen Risiko dan Otorisasi Federal (FedRAMP)
- Skalabilitas: Dengan AWS, Anda tidak perlu khawatir tentang kapasitas. Ketika kebutuhan Anda berubah, Anda dapat meningkatkan atau menurunkan konsumsi Anda tanpa overhead administratif.
- Biaya total kepemilikan (TCO) yang lebih rendah: Skala AWS operasi menurunkan biaya layanan dan membantu menurunkan TCO layanan. AWS AWS meneruskan penghematan biaya ini kepada pelanggan melalui penurunan harga.
- ay-as-you-go Harga P: Beli AWS layanan sesuai kebutuhan Anda dan hanya untuk periode yang Anda rencanakan untuk menggunakannya. AWS harga tidak memiliki biaya di muka, hukuman pemutusan hubungan kerja, atau kontrak jangka panjang.

Hasil bisnis yang ditargetkan

Tujuan dari panduan ini adalah untuk memberikan gambaran umumAWSlayanan yang dapat Anda gunakan untuk mendukung pendekatan pencadangan dan pemulihan untuk hal-hal berikut:

- Arsitektur lokal
- Arsitektur cloud-native
- Arsitektur hibrida
- Layanan native AWS
- Pemulihan bencana (DR)

Praktik dan pertimbangan terbaik tercakup bersama dengan ikhtisar layanan. Panduan ini juga memberi Anda pengorbanan antara menggunakan satu pendekatan di atas yang lain untuk cadangan dan pemulihan.

Memilih AWS layanan untuk perlindungan data

> **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 menyediakan sejumlah penyimpanan dan layanan pelengkap yang dapat digunakan sebagai bagian dari pendekatan pencadangan dan pemulihan Anda. Layanan ini dapat mendukung arsitektur cloud-native dan hybrid. Layanan yang berbeda lebih efektif untuk kasus penggunaan yang berbeda.

- Amazon S3 cocok untuk kasus penggunaan hybrid dan cloud-native. Ini menyediakan solusi penyimpanan objek tujuan umum yang sangat tahan lama yang cocok untuk mencadangkan file individual, server, atau seluruh pusat data.
- AWS Storage Gatewaysangat ideal untuk kasus penggunaan hibrida. Storage Gateway menggunakan kekuatan Amazon S3 untuk persyaratan pencadangan dan penyimpanan lokal yang umum. Aplikasi Anda terhubung ke layanan melalui mesin virtual (VM) atau perangkat gateway perangkat keras menggunakan protokol penyimpanan standar berikut:
  - Sistem File Jaringan (NFS)
  - Blok Pesan Server (SMB)
  - Antarmuka Sistem Komputer Kecil Internet (iSCSI)

  Gateway menjembatani protokol lokal umum ini ke layanan AWS penyimpanan seperti berikut:
  - Amazon S3
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway memudahkan penyediaan penyimpanan elastis dan berkinerja tinggi untuk file, volume, snapshot, dan kaset virtual. AWS
- AWS Backupadalah layanan pencadangan yang dikelola sepenuhnya untuk memusatkan dan mengotomatiskan cadangan data di seluruh AWS layanan. Dengan menggunakan AWS Backup, Anda dapat mengonfigurasi kebijakan pencadangan secara terpusat dan memantau aktivitas pencadangan untuk AWS sumber daya, seperti berikut ini:

  - Volume EBS
  - Instans EC2 (termasuk aplikasi Windows)
  - Basis data Amazon RDS dan Amazon Aurora
  - Tabel DynamoDB
  - Database Amazon Neptunus
  - Amazon DocumentDB (dengan kompatibilitas MongoDB) database
  - Sistem file Amazon EFS
  - Sistem file Amazon FSx for Lustre dan sistem file Amazon FSx for Windows File Server
  - Beban kerja VMware di tempat dan di VMware Cloud di AWS
  - Volume Storage Gateway

  Biaya AWS Backup didasarkan pada penyimpanan yang Anda konsumsi, pulihkan, dan transfer dalam sebulan. Untuk informasi lebih lanjut, lihat AWS Backup harga.

- AWS Elastic Disaster Recoveryterus mereplikasi mesin Anda ke area pementasan berbiaya rendah di AWS akun target Anda dan Wilayah pilihan Anda. Anda dapat menggunakan Elastic Disaster Recovery untuk premises-to-cloud DR dan Cross-region DR.
- AWS Configmemberikan tampilan terperinci tentang konfigurasi AWS sumber daya di AWS akun Anda. Ini termasuk bagaimana sumber daya terkait satu sama lain dan bagaimana mereka dikonfigurasi di masa lalu. Dalam tampilan ini, Anda dapat melihat bagaimana konfigurasi sumber daya dan hubungan telah berubah dari waktu ke waktu.

  Ketika Anda mengaktifkan perekaman AWS Config konfigurasi untuk AWS sumber daya Anda, Anda mempertahankan riwayat hubungan sumber daya Anda dari waktu ke waktu. Ini membantu mengidentifikasi dan melacak hubungan AWS sumber daya (termasuk sumber daya yang dihapus) hingga tujuh tahun. Misalnya, AWS Config dapat melacak hubungan volume snapshot Amazon EBS dan instans EC2 tempat volume dilampirkan.
- AWS Lambdadapat digunakan untuk mendefinisikan dan mengotomatiskan prosedur pencadangan dan pemulihan secara terprogram untuk beban kerja Anda. Anda dapat menggunakan AWS SDK untuk berinteraksi dengan AWS layanan dan datanya. Anda juga dapat menggunakan CloudWatch Acara Amazon untuk menjalankan fungsi Lambda Anda secara terjadwal.

AWS layanan menyediakan fitur khusus untuk pencadangan dan pemulihan. Untuk setiap AWS layanan yang Anda gunakan, konsultasikan AWS dokumentasi untuk menentukan fitur pencadangan, pemulihan, dan perlindungan data yang disediakan oleh layanan. Anda dapat menggunakan operasi

AWS Command Line Interface (AWS CLI), AWS SDK, dan API untuk mengotomatiskan fitur AWS khusus layanan untuk pencadangan dan pemulihan data.

Merancang solusi cadangan dan pemulihan

Saat mengembangkan strategi komprehensif untuk mencadangkan dan memulihkan data, Anda harus terlebih dahulu mengidentifikasi kemungkinan situasi kegagalan atau bencana dan potensi dampak bisnisnya. Di beberapa industri, Anda harus mempertimbangkan persyaratan peraturan untuk keamanan data, privasi, dan penyimpanan catatan.

Proses pencadangan dan pemulihan harus mencakup tingkat perincian yang sesuai untuk memenuhi tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO) untuk beban kerja dan proses bisnis pendukungnya, termasuk yang berikut ini:

- Pemulihan tingkat file (misalnya, file konfigurasi untuk aplikasi)
- Data aplikasi—tingkat pemulihan (misalnya, database tertentu dalam MySQL)
- Pemulihan tingkat aplikasi (misalnya, versi aplikasi server web tertentu)
- Pemulihan tingkat volume Amazon EC2 (misalnya, volume EBS)
- Pemulihan tingkat instans EC2. (misalnya, instans EC2)
- Pemulihan layanan terkelola (misalnya, tabel DynamoDB)

Pastikan untuk mempertimbangkan semua persyaratan pemulihan untuk solusi Anda dan dependensi data antara berbagai komponen dalam arsitektur Anda. Untuk memfasilitasi proses pemulihan yang sukses, koordinasikan cadangan dan pemulihan antara berbagai komponen dalam arsitektur Anda.

Topik berikut menjelaskan pendekatan pencadangan dan pemulihan berdasarkan organisasi infrastruktur Anda. Infrastruktur TI secara luas dapat dikategorikan sebagai lokal, hibrida, atau cloud native.

Backup dan pemulihan menggunakanAWS Backup

AWS Backupadalah layanan cadangan yang dikelola sepenuhnya memusatkan dan mengotomatisasi cadangan data di seluruhAWSlayanan.AWS Backupmenyediakan lapisan orkestrasi yang mengintegrasikan Amazon CloudWatch,AWS CloudTrail,AWS Identity and Access Management(IAM),AWS Organizations, dan layanan lainnya. Ini terpusat,AWSSolusi asli Cloud menyediakan kemampuan pencadangan global yang dapat membantu Anda mencapai persyaratan pemulihan bencana dan kepatuhan Anda. MenggunakanAWS Backup, Anda dapat mengonfigurasi kebijakan cadangan secara terpusat dan memantau aktivitas pencadanganAWSsumber daya.

AWS Backupadalah solusi ideal untuk menerapkan rencana cadangan standar untuk AndaAWSsumber daya di seluruhAWSakun dan Wilayah. KarenaAWS Backupmendukung beberapaAWSjenis sumber daya, itu membuat lebih mudah untuk mempertahankan dan menerapkan strategi cadangan untuk beban kerja menggunakan beberapaAWSsumber daya yang perlu didukung secara kolektif.AWS Backupjuga memungkinkan Anda untuk secara kolektif memantau operasi cadangan dan pemulihan yang melibatkan beberapaAWSsumber daya.

Jika Anda memiliki persyaratan kepatuhan dan audit, Anda dapat menggunakanAWS BackupAudit Managerfitur untuk membuat kerangka kerja audit dan laporan untuk mendukung persyaratan kepatuhan Anda. ParameterAWS BackupKunci VaultFitur juga mendukung persyaratan kepatuhan dengan menegakkan konfigurasi write-once, read-many (WORM) untuk semua backup Anda yang disimpan dalam lemari besi cadangan diAWS Backup.

Pembeda kunci untukAWS Backupadalah dukungan untuk Organizations. Dengan menggunakan dukungan ini, Anda dapat menentukan dan mengelola kebijakan cadangan di tingkat organisasi atau unit organisasi dan secara otomatis menerapkan kebijakan tersebut untuk setiap terkaitAWSakun dan Wilayah. Seperti yang Anda onboard baruAWSakun dan Wilayah, Anda tidak perlu menentukan dan mengelola paket cadangan secara terpisah.

AWS Backupdapat mempermudah Anda mengimplementasikan kebijakan pencadangan di seluruh organisasi dengan menggunakan tag. Anda dapat membuat paket cadangan terpisah yang masing-masing memiliki pengaturan frekuensi dan retensi unik dan kemudian membuat tag pasangan nilai kunci unik yang memilih sumber daya yang akan disertakan untuk cadangan.

Misalnya, Anda dapat membuat paket cadangan harian yang memulai cadangan pada pukul 05:00 UTC setiap hari dan memiliki kebijakan retensi 35 hari. Rencana cadangan ini dapat mencakuppenugasan sumber daya cadanganyang menentukan bahwa setiap didukungAWSsumber daya dengan kunci tagcadangandan nilai tagharianakan didukung sesuai dengan rencana ini.

Selain itu, Anda dapat membuat paket cadangan bulanan yang dimulai pada pukul 05:00 UTC pada hari pertama setiap bulan dan memiliki kebijakan retensi 366 hari. Rencana cadangan ini dapat mencakup penugasan sumber daya cadangan yang menentukan bahwa setiap didukungAWSsumber daya dengan kunci tagcadangandan nilai tagbulananakan didukung sesuai dengan rencana ini.

Anda kemudian dapat menggunakan kebijakan tag dandiperlukan-tag AWS Configaturan untuk memastikan bahwa semuaAWSsumber daya yang didukung memiliki kunci tag ini dan salah satu nilai tag ini. Pendekatan ini dapat membantu Anda secara konsisten menerapkan dan mempertahankan pendekatan cadangan standarAWSuntuk didukungAWS Backupsumber daya. Anda dapat memperluas pendekatan ini untuk standarisasi backup untuk aplikasi Anda dan lapisan arsitektur yang memiliki tujuan titik pemulihan (RPO) persyaratan yang berbeda.

Sebaiknya ambil langkah untuk mengamankan brankas cadangan Anda. Misalnya, Anda dapat menerapkan kebijakan kontrol layanan Organizations (SCP) yang mencegah penyimpanan cadangan dihapus atau dibagikan dengan yang tidak diinginkanAWSakun. Untuk rincian lebih lanjut dan pertimbangan keamanan penting lainnya, tinjauPraktik terbaik keamanan untuk mengamankan cadangan diAWSposting blog.

AWS Backupdapat menyederhanakan implementasi rencana pemulihan bencana (DR)AWSkarena mendukung beberapaAWSsumber daya yang dapat ditangani secara kolektif. Misalnya, Anda dapat menerapkanLintas-Wilayahdanlintas-akuncadangan untuk sebagian besarAWSjenis sumber daya yang didukung olehAWS Backup. Cadangan lintas akun meningkatkan keamanan cadangan karena salinan tersedia di akun terpisah. Cadangan Lintas Wilayah meningkatkan ketersediaan karena cadangan tersedia di lebih dari satu Wilayah. Untuk detail tentang didukungAWSjenis sumber daya, lihatKetersediaan fitur berdasarkan sumber dayatabel.

Anda dapat menggunakan contohBackup dan Pemulihan denganAWS Backupsolusi sumber terbukauntuk menerapkan infrastruktur sebagai kode (IAC) dan integrasi berkelanjutan dan berkelanjutan pengiriman (CI/CD) pendekatan untuk mengelola backup untuk AndaAWS Organizationsorganisasi. Solusi ini mencakup fitur khusus, seperti menerapkan kembali secara otomatisAWStag pada dipulihkanAWSsumber daya serta membangun kubah cadangan sekunder di akun terpisah dan Wilayah untuk tujuan DR.

Backup dan pemulihan menggunakan Amazon S3

Anda dapat menggunakan Amazon Simple Storage Service (Amazon S3) untuk menyimpan dan mengambil data dalam jumlah berapa pun, kapan saja. Anda dapat menggunakan Amazon S3 sebagai penyimpanan tahan lama untuk data aplikasi dan proses pencadangan dan pemulihan tingkat file. Misalnya, Anda dapat menyalin cadangan database dari instance database ke Amazon S3 dengan skrip cadangan menggunakan AWS CLI atau SDK. AWS

Layanan AWS gunakan Amazon S3 untuk penyimpanan yang sangat tahan lama dan andal, seperti pada contoh berikut:

- Amazon EC2 menggunakan Amazon S3 untuk menyimpan snapshot Amazon EBS untuk volume EBS dan untuk toko instans EC2.
- Storage Gateway terintegrasi dengan Amazon S3 untuk menyediakan lingkungan lokal dengan berbagi file, volume, dan pustaka tape yang didukung Amazon S3.
- Amazon RDS menggunakan Amazon S3 untuk snapshot database.

Banyak solusi cadangan pihak ketiga juga menggunakan Amazon S3. Misalnya, Perlindungan Data Terpadu Arcserve mendukung Amazon S3 untuk pencadangan server lokal dan cloud-native yang tahan lama.

Anda dapat menggunakan fitur terintegrasi Amazon S3 dari layanan ini untuk menyederhanakan pendekatan pencadangan dan pemulihan Anda. Pada saat yang sama, Anda bisa mendapatkan keuntungan dari daya tahan tinggi dan ketersediaan yang disediakan oleh Amazon S3.

Amazon S3 menyimpan data sebagai objek dalam sumber daya yang disebut bucket. Anda dapat menyimpan benda sebanyak yang Anda inginkan dalam ember. Anda dapat menulis, membaca, dan menghapus objek di bucket Anda dengan kontrol akses berbutir halus. Objek tunggal bisa berukuran hingga 5 TB.

Menggunakan kelas penyimpanan Amazon S3 untuk mengurangi biaya penyimpanan data cadangan

Amazon S3 menawarkan beberapa kelas penyimpanan untuk digunakan dalam arsitektur lokal, hibrida, dan cloud-native. Semua kelas penyimpanan menyediakan kapasitas yang dapat diskalakan yang tidak memerlukan manajemen volume atau media seiring bertambahnya kumpulan data

cadangan Anda. Model pay-for-what-you -use dan biaya rendah per GB/bulan membuat kelas penyimpanan Amazon S3 cocok untuk berbagai kasus penggunaan perlindungan data. Kelas penyimpanan Amazon S3 dirancang untuk kasus penggunaan yang berbeda, termasuk kategori berikut:

- Kelas penyimpanan akses yang sering untuk penyimpanan tujuan umum dari data yang sering diakses (misalnya, file konfigurasi, cadangan yang tidak direncanakan, cadangan harian). Ini termasuk kelas penyimpanan Standar S3, yang merupakan default untuk semua objek Amazon S3.
- Kelas penyimpanan akses yang jarang untuk data yang berumur panjang, tetapi jarang diakses (misalnya, cadangan bulanan). Ini termasuk kelas penyimpanan IA Standar S3. IA adalah singkatan dari akses jarang.
- Kelas penyimpanan S3 Glacier untuk data yang berumur sangat panjang yang jarang perlu diakses (misalnya, cadangan tahunan). Ini termasuk S3 Glacier Deep Archive, yang menyediakan penyimpanan dengan biaya terendah. AWS

Untuk backup dengan pola akses yang tidak diketahui atau berubah, Anda dapat menggunakan kelas penyimpanan S3 Intelligent-Tiering. S3 Intelligent-Tiering secara otomatis mentransisikan objek ke tingkat yang paling hemat biaya berdasarkan berapa hari yang lalu sebuah objek terakhir diakses.

> **Note**
>
> Beberapa kelas penyimpanan memiliki biaya durasi minimum. Untuk detailnya, lihat harga Amazon S3, dan gunakan pencarian halaman web untuk menemukannya. `duration`

Amazon S3 menawarkan kebijakan siklus hidup yang dapat Anda konfigurasikan untuk mengelola data sepanjang siklus hidupnya. Setelah kebijakan disetel, data Anda akan dimigrasi secara otomatis ke kelas penyimpanan yang sesuai tanpa perubahan apa pun pada aplikasi Anda. Untuk informasi selengkapnya, lihat dokumentasi manajemen siklus hidup objek Amazon S3.

Untuk mengurangi biaya pencadangan, gunakan pendekatan kelas penyimpanan berjenjang berdasarkan tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO) Anda, seperti pada contoh berikut:

- Pencadangan harian selama 2 minggu terakhir menggunakan Standar S3
- Pencadangan mingguan selama 3 bulan terakhir menggunakan IA Standar S3
- Pencadangan triwulanan untuk tahun lalu di S3 Glacier Flexible Retrieval

- Pencadangan tahunan selama 5 tahun terakhir di S3 Glacier Deep Archive
- Cadangan dihapus dari S3 Glacier Deep Archive setelah tanda 5 tahun

Membuat bucket S3 standar untuk cadangan dan arsip

Anda dapat membuat bucket S3 standar untuk pencadangan dan pengarsipan dengan kebijakan pencadangan dan penyimpanan perusahaan Anda yang diterapkan melalui kebijakan siklus hidup S3. Penandaan dan pelaporan alokasi biaya untuk AWS penagihan didasarkan pada tag yang ditetapkan di tingkat bucket. Jika alokasi biaya penting, buat cadangan terpisah dan arsipkan ember S3 untuk setiap proyek atau unit bisnis sehingga Anda dapat mengalokasikan biaya yang sesuai.

Skrip dan aplikasi cadangan Anda dapat menggunakan bucket S3 cadangan dan arsip yang Anda buat untuk menyimpan point-in-time snapshot untuk data aplikasi dan beban kerja. Anda dapat membuat awalan S3 standar untuk membantu Anda mengatur snapshot point-in-time data Anda. Misalnya, jika Anda membuat cadangan per jam, pertimbangkan untuk menggunakan awalan cadangan seperti. `YYYY/MM/DD/HH/<WorkloadName>/<files...>` Dengan melakukan ini, Anda dapat dengan cepat mengambil point-in-time cadangan Anda secara manual atau terprogram.

Menggunakan versi Amazon S3 untuk secara otomatis mempertahankan riwayat rollback

Anda dapat mengaktifkan versi objek S3 untuk mempertahankan riwayat perubahan objek, termasuk kemampuan untuk kembali ke versi sebelumnya. Ini berguna untuk file konfigurasi dan objek lain yang mungkin berubah lebih sering daripada jadwal point-in-time cadangan Anda. Ini juga berguna untuk file yang harus dikembalikan satu per satu.

Menggunakan Amazon S3 untuk mencadangkan dan memulihkan file konfigurasi khusus untuk AMI

Amazon S3 dengan versi objek dapat menjadi sistem catatan Anda untuk konfigurasi beban kerja dan file opsi Anda. Misalnya, Anda mungkin menggunakan gambar AWS Marketplace Amazon EC2 standar yang dikelola oleh ISV. Gambar ini mungkin berisi perangkat lunak yang konfigurasinya dipertahankan dalam sejumlah file konfigurasi. Anda dapat mempertahankan file konfigurasi khusus Anda di Amazon S3. Saat instans diluncurkan, Anda dapat menyalin file konfigurasi ini ke instans sebagai bagian dari data pengguna instans Anda. Saat menerapkan pendekatan ini, Anda tidak perlu menyesuaikan dan membuat ulang AMI untuk menggunakan versi yang diperbarui.

Menggunakan Amazon S3 dalam proses pencadangan dan pemulihan kustom Anda

Amazon S3 menyediakan penyimpanan cadangan tujuan umum yang dapat Anda integrasikan dengan cepat ke dalam proses pencadangan kustom yang ada. Anda dapat menggunakan operasi AWS CLI, AWS SDK, dan API untuk mengintegrasikan skrip dan proses pencadangan dan pemulihan yang menggunakan Amazon S3. Misalnya, Anda mungkin memiliki skrip cadangan database yang melakukan ekspor database setiap malam. Anda dapat menyesuaikan skrip ini untuk menyalin cadangan malam Anda ke Amazon S3 untuk penyimpanan di luar kantor. Lihat Batch upload file ke cloud tutorial untuk gambaran umum tentang cara melakukannya.

Anda dapat mengambil pendekatan serupa untuk mengekspor dan mencadangkan data untuk aplikasi yang berbeda berdasarkan RPO masing-masing. Selain itu, Anda dapat menggunakan AWS Systems Manager untuk menjalankan skrip cadangan pada instans terkelola Anda. Systems Manager menyediakan otomatisasi, kontrol akses, penjadwalan, pencatatan, dan pemberitahuan untuk proses pencadangan individual Anda.

Mengamankan data cadangan di Amazon S3

Keamanan data adalah masalah universal, dan AWS menangani keamanan dengan sangat serius. Keamanan adalah dasar dari setiap Layanan AWS. Amazon S3 menyediakan kemampuan untuk kontrol akses dan enkripsi baik saat istirahat maupun dalam perjalanan. Semua endpoint Amazon S3 mendukung SSL/TLS untuk mengenkripsi data dalam perjalanan. Anda dapat mengatur enkripsi untuk objek saat istirahat dengan melakukan hal berikut:

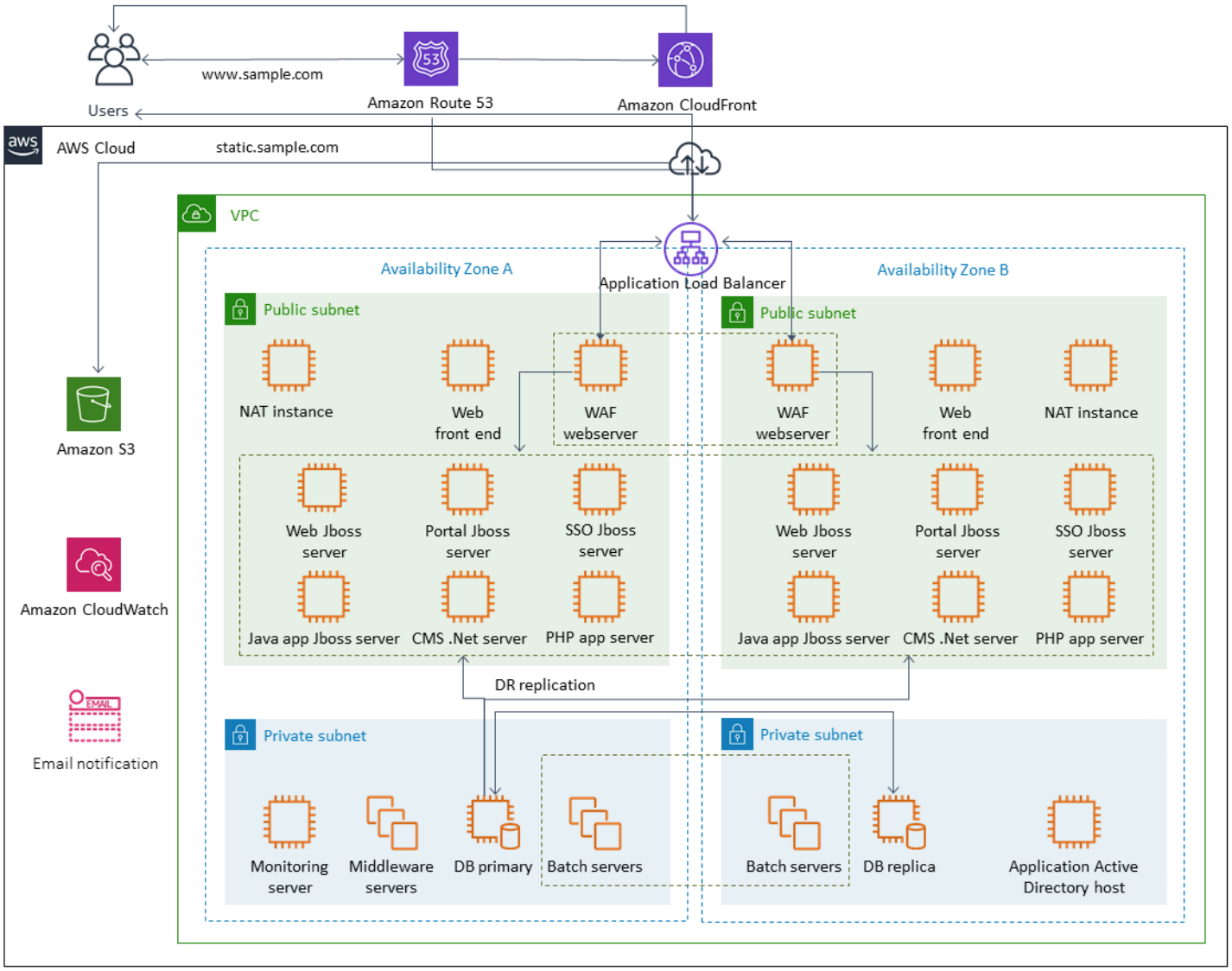
- Menggunakan enkripsi sisi server dengan kunci enkripsi terkelola Amazon S3 (default)
- Menggunakan enkripsi sisi server dengan kunci AWS Key Management Service (AWS KMS) yang disimpan di AWS KMS
- Menggunakan enkripsi sisi klien

Anda dapat menggunakan AWS Identity and Access Management (IAM) untuk mengontrol akses ke objek S3. IAM memberikan kontrol atas izin untuk objek individual dan jalur awalan tertentu dalam bucket S3. Anda dapat mengaudit akses ke objek S3 dengan menggunakan logging tingkat objek dengan. AWS CloudTrail

Backup dan pemulihan untuk Amazon EC2 dengan volume EBS

AWS menyediakan beberapa metode untuk mencadangkan instans Amazon EC2 Anda. Bagian ini mencakup berbagai aspek pencadangan volume Amazon Elastic Block Store (Amazon EBS) atau volume penyimpanan instans untuk penyimpanan. Pertimbangkan AWS Backup sebagai pilihan pertama Anda untuk mengelola cadangan AWS jika memenuhi persyaratan Anda. Ingatlah bahwa cadangan hanya baik jika mereka dapat dikembalikan ke fungsi yang dimaksudkan. Fungsi pemulihan dan pemulihan harus diuji secara teratur untuk mengonfirmasi hal ini.

Arsitektur solusi dalam diagram berikut menjelaskan lingkungan beban kerja yang sepenuhnya ada AWS dengan sebagian besar arsitektur berdasarkan Amazon EC2. Seperti gambar berikut menunjukkan, skenario termasuk server web, server aplikasi, server pemantauan, database, dan Active Directory.



AWS menyediakan banyak layanan berfitur lengkap untuk banyak server Amazon EC2 yang diwakili dalam arsitektur ini untuk melakukan pekerjaan yang tidak terdiferensiasi dalam membuat, menyediakan, mencadangkan, memulihkan, dan mengoptimalkan instans dan penyimpanan. Pertimbangkan apakah layanan ini masuk akal dalam arsitektur Anda untuk mengurangi kompleksitas dan manajemen. AWS juga menyediakan layanan untuk meningkatkan ketersediaan arsitektur berbasis Amazon EC2 Anda. Secara khusus, pertimbangkan Auto Scaling Amazon EC2 dan Elastic Load Balancing untuk melengkapi beban kerja Anda di Amazon EC2. Menggunakan layanan ini dapat meningkatkan ketersediaan dan toleransi kesalahan arsitektur Anda dan membantu Anda memulihkan instans yang rusak dengan dampak pengguna minimal.

Instans EC2 terutama menggunakan volume Amazon EBS untuk penyimpanan persisten. Amazon EBS menyediakan sejumlah fitur untuk pencadangan dan pemulihan yang dibahas secara rinci di bagian ini.

Topik

- Pencadangan dan pemulihan Amazon EC2 dengan snapshot dan AMI
- Membuat cadangan volume EBS dengan snapshot AMI dan EBS
- Memulihkan volume Amazon EBS atau instans EC2

Pencadangan dan pemulihan Amazon EC2 dengan snapshot dan AMI

Pertimbangkan apakah Anda perlu membuat cadangan lengkap instans EC2 dengan Amazon Machine Image (AMI) atau mengambil snapshot dari volume individual.

Menggunakan snapshot AMI atau Amazon EBS untuk cadangan

AMI mencakup yang berikut ini:

- Satu atau lebih snapshot. Saya nstance-store-backed AMI menyertakan template untuk volume root instance (misalnya, sistem operasi, server aplikasi, dan aplikasi).
- Luncurkan izin yang mengontrol AWS akun mana yang dapat menggunakan AMI untuk meluncurkan instance.
- Pemetaan perangkat blok yang menentukan volume yang akan dilampirkan ke instance saat diluncurkan.

Anda dapat menggunakan AMI untuk meluncurkan instance baru dengan perangkat lunak dan data yang telah dikonfigurasi sebelumnya. Anda dapat membuat AMI saat Anda ingin membuat baseline, yang merupakan konfigurasi yang dapat digunakan kembali untuk meluncurkan lebih banyak instance. Saat Anda membuat AMI dari instans EC2 yang ada, snapshot diambil untuk semua volume yang dilampirkan ke instance. Snapshot mencakup pemetaan perangkat.

Anda tidak dapat menggunakan snapshot untuk meluncurkan instance baru, tetapi Anda dapat menggunakannya untuk mengganti volume pada instance yang ada. Jika Anda mengalami kerusakan data atau kegagalan volume, Anda dapat membuat volume dari snapshot yang telah Anda

ambil dan mengganti volume lama. Anda juga dapat menggunakan snapshot untuk menyediakan volume baru dan melampirkannya selama peluncuran instance baru.

Jika Anda menggunakan AMI platform dan aplikasi yang dikelola dan dipublikasikan oleh AWS atau dari AWS Marketplace, pertimbangkan untuk mempertahankan volume terpisah untuk data Anda. Anda dapat mencadangkan volume data Anda sebagai snapshot yang terpisah dari sistem operasi dan volume aplikasi. Kemudian gunakan snapshot volume data dengan AMI yang baru diperbarui yang diterbitkan oleh AWS atau dari file. AWS Marketplace Pendekatan ini memerlukan pengujian dan perencanaan yang cermat untuk mencadangkan dan memulihkan semua data kustom, termasuk informasi konfigurasi, pada AMI yang baru diterbitkan.

Proses pemulihan dipengaruhi oleh pilihan Anda antara cadangan AMI atau cadangan snapshot. Jika Anda membuat AMI untuk dijadikan cadangan instans, Anda harus meluncurkan instans EC2 dari AMI sebagai bagian dari proses pemulihan Anda. Anda mungkin juga perlu mematikan instance yang ada untuk menghindari potensi tabrakan. Contoh tabrakan potensial adalah pengidentifikasi keamanan (SID) untuk instance Windows yang bergabung dengan domain. Proses pemulihan untuk snapshot mungkin mengharuskan Anda melepaskan volume yang ada dan melampirkan volume yang baru dipulihkan. Atau Anda mungkin perlu membuat perubahan konfigurasi untuk mengarahkan aplikasi Anda ke volume yang baru dilampirkan.

AWS Backup mendukung pencadangan tingkat instance sebagai AMI dan pencadangan tingkat volume sebagai snapshot terpisah:

- Untuk cadangan lengkap semua volume EBS pada instance, buat AMI dari instans EC2 yang berjalan di Linux atau Windows. Saat Anda ingin memutar kembali, gunakan wizard instance peluncuran untuk membuat instance. Di wizard peluncuran instance, pilih AMI Saya.
- Untuk mencadangkan volume individual, buat snapshot. Untuk mengembalikan snapshot, lihat Membuat volume dari snapshot. Anda dapat menggunakan AWS Management Console atau AWS Command Line Interface (AWS CLI).

Biaya instance AMI adalah penyimpanan semua volume pada instance, tetapi bukan metadata. Biaya untuk snapshot EBS adalah penyimpanan volume individu. Untuk informasi selengkapnya tentang biaya penyimpanan volume, lihat halaman harga Amazon EBS.

Volume server

Volume EBS adalah opsi penyimpanan persisten utama untuk Amazon EC2. Anda dapat menggunakan penyimpanan blok ini untuk data terstruktur, seperti database, atau data tidak terstruktur, seperti file dalam sistem file pada volume.

Volume EBS ditempatkan di Availability Zone tertentu. Volume direplikasi di beberapa server untuk mencegah hilangnya data dari kegagalan komponen tunggal. Kegagalan mengacu pada kehilangan volume total atau sebagian, tergantung pada ukuran dan kinerja volume.

Volume EBS dirancang untuk tingkat kegagalan tahunan (AFR) sebesar 0,1-0,2 persen. Ini membuat volume EBS 20 kali lebih andal daripada disk drive komoditas biasa, yang gagal dengan AFR sekitar 4 persen. Misalnya, jika Anda memiliki 1.000 volume EBS yang berjalan selama 1 tahun, Anda harus mengharapkan satu atau dua volume akan mengalami kegagalan.

Amazon EBS juga mendukung fitur snapshot untuk mengambil point-in-time cadangan data Anda. Semua jenis volume EBS menawarkan kemampuan snapshot yang tahan lama dan dirancang untuk ketersediaan 99,999 persen. Untuk informasi selengkapnya, lihat Perjanjian Tingkat Layanan Komputasi Amazon.

Amazon EBS menyediakan kemampuan untuk membuat snapshot (backup) dari volume EBS apa pun. Snapshot adalah fitur dasar untuk membuat cadangan volume EBS Anda. Sebuah snapshot mengambil salinan volume EBS dan menempatkannya di Amazon S3, di mana ia disimpan secara berlebihan di beberapa Availability Zone. Snapshot awal adalah salinan lengkap volume; snapshot yang sedang berlangsung hanya menyimpan perubahan tingkat blok tambahan. Lihat dokumentasi Amazon EC2 untuk detail tentang cara membuat snapshot Amazon EBS.

Anda dapat melakukan operasi pemulihan, menghapus snapshot, atau memperbarui metadata snapshot, seperti tag, yang terkait dengan snapshot dari konsol Amazon EC2 di Wilayah yang sama dengan yang Anda ambil snapshot.

Memulihkan snapshot akan membuat volume Amazon EBS baru dengan data volume penuh. Jika Anda hanya memerlukan pemulihan sebagian, Anda dapat melampirkan volume ke instance yang sedang berjalan di bawah nama perangkat yang berbeda. Kemudian pasang, dan gunakan perintah salin sistem operasi untuk menyalin data dari volume cadangan ke volume produksi.

Snapshot Amazon EBS juga dapat disalin antar AWS Wilayah dengan menggunakan kemampuan menyalin snapshot Amazon EBS, seperti yang dijelaskan dalam dokumentasi Amazon EC2. Anda dapat menggunakan fitur ini untuk menyimpan cadangan Anda di Wilayah lain tanpa harus mengelola teknologi replikasi yang mendasarinya.

Menetapkan volume server terpisah

Anda mungkin sudah menggunakan satu set standar volume terpisah untuk sistem operasi, log, aplikasi, dan data. Dengan menetapkan volume server terpisah, Anda dapat mengurangi cakupan dampak ketika ada kegagalan aplikasi atau platform yang disebabkan oleh kelelahan ruang disk. Risiko ini biasanya lebih besar dengan hard drive fisik, karena Anda tidak memiliki fleksibilitas untuk memperluas volume dengan cepat. Dengan drive fisik, Anda harus membeli drive baru, mencadangkan data, dan kemudian mengembalikan data pada drive baru. Dengan AWS, risiko ini sangat berkurang karena Anda dapat menggunakan Amazon EBS untuk memperluas volume yang disediakan. Lihat informasi yang lebih lengkap dalam dokumentasi AWS.

Pertahankan volume terpisah untuk data aplikasi, data pengguna, log, dan file swap sehingga Anda dapat menggunakan kebijakan pencadangan dan pemulihan terpisah untuk sumber daya ini. Dengan memisahkan volume untuk data Anda, Anda juga dapat menggunakan jenis volume yang berbeda berdasarkan kinerja dan persyaratan penyimpanan untuk data. Anda kemudian dapat mengoptimalkan dan menyempurnakan biaya Anda untuk beban kerja yang berbeda.

Pertimbangan misalnya volume toko

penyimpanan instans menyediakan penyimpanan tingkat blok sementara untuk instans Anda. Penyimpanan ini terletak pada disk yang secara fisik terpasang pada komputer host. Penyimpanan instans ideal untuk penyimpanan sementara informasi yang sering berubah, seperti buffer, cache, data awal, dan konten sementara lainnya. Mereka juga lebih disukai untuk data yang direplikasi di seluruh armada instance, seperti kumpulan server web yang seimbang beban.

Data dalam penyimpanan instans hanya bertahan selama masaterkait. Jika suatu instans me-reboot (secara sengaja atau tidak sengaja), data pada saat penyimpanan tetap ada. Namun, data di penyimpanan instance hilang dalam salah satu keadaan berikut.

- Drive yang mendasarinya gagal.
- Contoh tersebut berhenti.
- Instans berakhir

Oleh karena itu, jangan mengandalkan penyimpanan instance untuk data jangka panjang yang berharga. Sebaliknya, gunakan penyimpanan data yang lebih tahan lama, seperti Amazon S3, Amazon EBS, atau Amazon EFS.

Strategi umum dengan volume penyimpanan instans adalah menyimpan data yang diperlukan ke Amazon S3 secara teratur sesuai kebutuhan, berdasarkan tujuan titik pemulihan (RPO) dan tujuan waktu pemulihan (RTO). Anda kemudian dapat mengunduh data dari Amazon S3 ke penyimpanan instans Anda saat instance baru diluncurkan. Anda juga dapat mengunggah data ke Amazon S3 sebelum instance dihentikan. Untuk persistensi, buat volume EBS, lampirkan ke instans Anda, dan salin data dari volume penyimpanan instans ke volume EBS secara berkala. Untuk informasi selengkapnya, lihat Pusat Pengetahuan AWS.

Menandai dan menegakkan standar untuk snapshot EBS dan AMI

Menandai semua AWS sumber daya Anda adalah praktik penting untuk alokasi biaya, audit, pemecahan masalah, dan pemberitahuan. Penandaan penting untuk volume EBS sehingga informasi terkait yang diperlukan untuk mengelola dan memulihkan volume hadir. Tag tidak secara otomatis disalin dari instans EC2 ke AMI atau dari volume sumber ke snapshot. Pastikan proses pencadangan Anda menyertakan tag yang relevan dari sumber-sumber ini. Ini membantu Anda mengatur metadata snapshot, seperti kebijakan akses, informasi lampiran, dan alokasi biaya, untuk menggunakan cadangan ini di masa mendatang. Untuk informasi lebih lanjut tentang menandai AWS sumber daya Anda, lihat tagging best practices technical paper.

Selain tag yang Anda gunakan untuk semua AWS sumber daya, gunakan tag khusus cadangan berikut:

- ID contoh sumber
- ID volume sumber (untuk snapshot)
- Deskripsi titik pemulihan

Anda dapat menerapkan kebijakan penandaan dengan menggunakan AWS Config aturan dan izin IAM. IAM mendukung penggunaan tag yang diterapkan, sehingga Anda dapat menulis kebijakan IAM yang mengamanatkan penggunaan tag tertentu saat bertindak pada snapshot Amazon EBS. Jika `CreateSnapshot` operasi dicoba tanpa tag yang ditentukan dalam kebijakan izin IAM memberikan hak, pembuatan snapshot gagal dengan akses ditolak. Untuk informasi selengkapnya, lihat posting blog tentang menandai snapshot Amazon EBS tentang pembuatan dan menerapkan kebijakan keamanan yang lebih kuat.

Anda dapat menggunakan AWS Config aturan untuk mengevaluasi pengaturan konfigurasi AWS sumber daya Anda secara otomatis. Untuk membantu Anda memulai, AWS Config berikan aturan yang dapat disesuaikan dan telah ditentukan sebelumnya yang disebut aturan terkelola. Anda juga

dapat membuat aturan kustom Anda sendiri. Sementara AWS Config terus melacak perubahan konfigurasi di antara sumber daya Anda, ia memeriksa apakah perubahan ini melanggar salah satu kondisi dalam aturan Anda. Jika sumber daya melanggar aturan, AWS Config tandai sumber daya dan aturan sebagai tidak patuh. Perhatikan bahwa aturan terkelola tag yang diperlukan saat ini tidak mendukung snapshot dan AMI.

Membuat cadangan volume EBS dengan snapshot AMI dan EBS

AWS menyediakan banyak opsi untuk membuat dan mengelola AMI dan snapshot. Anda dapat menggunakan pendekatan yang memenuhi kebutuhan Anda. Masalah umum yang dihadapi banyak pelanggan adalah mengelola siklus hidup snapshot dan menyelaraskan snapshot dengan jelas berdasarkan tujuan, kebijakan retensi, dll. Tanpa penandaan yang tepat, ada risiko bahwa snapshot mungkin dihapus secara tidak sengaja atau sebagai bagian dari proses pembersihan otomatis. Anda mungkin juga akhirnya membayar untuk snapshot usang yang dipertahankan karena tidak ada pemahaman yang jelas apakah mereka masih diperlukan.

Mempersiapkan volume EBS sebelum membuat snapshot atau AMI

Sebelum Anda mengambil snapshot atau membuat AMI, buat persiapan yang diperlukan untuk volume EBS Anda. Membuat AMI menghasilkan snapshot baru untuk setiap volume EBS yang dilampirkan ke instance, jadi persiapan ini juga berlaku untuk AMI.

Anda dapat mengambil snapshot dari volume EBS terlampir yang digunakan oleh instans EC2 yang diaktifkan. Namun, snapshot hanya menangkap data yang telah ditulis ke volume EBS Anda pada saat perintah snapshot dikeluarkan. Ini mungkin mengecualikan data apa pun yang telah di-cache oleh aplikasi atau sistem operasi. Praktik terbaik adalah memiliki sistem dalam keadaan di mana ia tidak melakukan I/O. Idealnya, mesin tidak menerima lalu lintas dan dalam keadaan berhenti, tetapi ini jarang terjadi karena operasi TI 24/7 menjadi norma. Jika Anda dapat menyiram data apa pun dari memori sistem ke disk yang digunakan oleh aplikasi Anda dan menjeda file apa pun yang menulis ke volume cukup lama untuk mengambil snapshot, snapshot Anda harus lengkap.

Untuk membuat cadangan yang bersih, Anda harus menghapus database atau sistem file. Cara Anda melakukan ini tergantung pada database atau sistem file Anda.

Proses untuk database adalah sebagai berikut:

1. Jika memungkinkan, masukkan database ke mode cadangan panas.
2. Jalankan perintah snapshot Amazon EBS.

3. Keluarkan database dari mode cadangan panas atau, jika menggunakan replika baca, hentikan instance replika baca.

Proses untuk sistem file serupa, tetapi itu tergantung pada kemampuan sistem operasi atau sistem file. Misalnya, XFS adalah sistem file yang dapat menyiram datanya untuk cadangan yang konsisten. Untuk informasi selengkapnya, lihat xfs_freeze. Atau, Anda dapat memfasilitasi proses ini dengan menggunakan manajer volume logis yang mendukung pembekuan I/O.

Namun, jika Anda tidak dapat menyiram atau menjeda semua penulisan file ke volume, lakukan hal berikut:

1. Lepaskan volume dari sistem operasi.
2. Keluarkan perintah snapshot.
3. Remount volume untuk mencapai snapshot yang konsisten dan lengkap. Anda dapat melakukan remount dan menggunakan volume Anda saat status snapshot tertunda.

Proses snapshot berlanjut di latar belakang dan pembuatan snapshot cepat dan menangkap titik waktu. Volume yang Anda cadangkan dilepas hanya dalam hitungan detik. Anda dapat menjadwalkan jendela cadangan kecil di mana pemadaman diharapkan dan ditangani oleh klien dengan anggun.

Saat Anda membuat snapshot untuk volume EBS yang berfungsi sebagai perangkat root, hentikan instance sebelum mengambil snapshot. Windows menyediakan Volume Shadow Copy Service (VSS) untuk membantu membuat snapshot yang konsisten dengan aplikasi. AWS menyediakan dokumen Systems Manager yang dapat Anda jalankan untuk mengambil cadangan tingkat gambar dari aplikasi sadar VSS. Snapshot mencakup data dari transaksi yang tertunda antara aplikasi ini dan disk. Anda tidak perlu mematikan instans Anda atau memutuskannya saat Anda mencadangkan semua volume terlampir. Lihat informasi yang lebih lengkap dalam dokumentasi AWS.

> **Note**
>
> Jika Anda membuat AMI Windows sehingga Anda dapat menerapkan instance serupa lainnya, gunakan EC2config atau EC2launch untuk Sysprep instance Anda. Kemudian buat AMI dari instance yang dihentikan. Sysprep menghapus informasi unik dari instans Windows Amazon EC2, termasuk SID, nama komputer, dan driver. Duplikat SID dapat menyebabkan masalah dengan Active Directory, Windows Server Update Services (WSUS), masalah login, aktivasi tombol volume Windows, Microsoft Office, dan produk pihak ketiga. Jangan gunakan

Sysprep dengan instans Anda jika AMI Anda untuk tujuan pencadangan dan Anda ingin memulihkan instance yang sama dengan semua informasi uniknya yang utuh.

Membuat snapshot volume EBS secara manual dari konsol

Buat snapshot dari volume yang sesuai atau seluruh instance sebelum Anda membuat perubahan besar yang belum sepenuhnya diuji pada instance. Misalnya, Anda mungkin ingin membuat snapshot sebelum memutakhirkan atau menambal aplikasi atau perangkat lunak sistem pada instans Anda.

Anda dapat membuat snapshot secara manual dari konsol. Di konsol Amazon EC2, pada halaman Volume Toko Blok Elastis, pilih volume yang ingin Anda cadangkan. Kemudian pada menu Actions, pilih Create Snapshot. Anda dapat mencari volume yang dilampirkan ke instance tertentu dengan memasukkan ID instans di kotak filter.

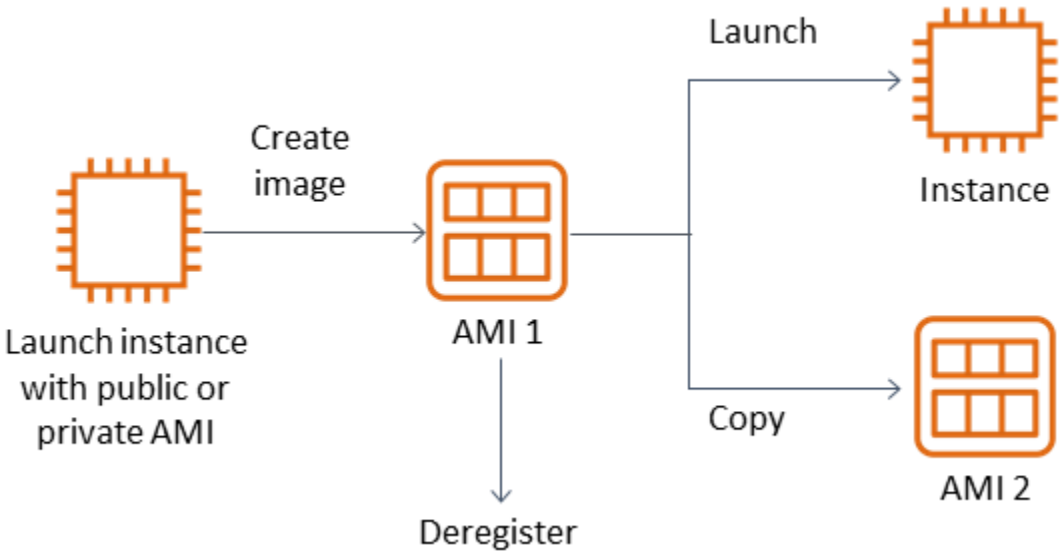
Masukkan deskripsi dan tambahkan tag yang sesuai. Tambahkan `Name` tag untuk mempermudah menemukan volume nanti. Tambahkan tag lain yang sesuai berdasarkan strategi penandaan Anda.

Membuat AMI

AMI menyediakan informasi yang diperlukan untuk meluncurkan instance. AMI menyertakan volume root dan snapshot dari volume EBS yang dilampirkan ke instance saat gambar dibuat. Anda tidak dapat meluncurkan instans baru dari snapshot EBS saja; Anda harus meluncurkan instans baru dari AMI.

Saat Anda membuat AMI, AMI dibuat di akun dan Wilayah yang Anda gunakan. Proses pembuatan AMI membuat snapshot Amazon EBS untuk setiap volume yang dilampirkan ke instance, dan AMI mengacu pada snapshot Amazon EBS ini. Snapshot ini berada di Amazon S3 dan sangat tahan lama.

Setelah membuat AMI instans EC2, Anda dapat menggunakan AMI untuk membuat ulang instans atau meluncurkan lebih banyak salinan instans. Anda juga dapat menyalin AMI dari satu Wilayah ke Wilayah lain untuk migrasi aplikasi atau DR.



AMI harus dibuat dari instans EC2 kecuali Anda memigrasikan mesin virtual, seperti mesin virtual VMWARE, ke. AWS Untuk membuat AMI dari konsol Amazon EC2, pilih instans, pilih Tindakan, pilih Gambar, lalu pilih Buat Gambar.

Amazon Data Lifecycle Manager

Untuk mengotomatiskan pembuatan, penyimpanan, dan penghapusan snapshot Amazon EBS, Anda dapat menggunakan Amazon Data Lifecycle Manager. Mengotomatiskan manajemen snapshot membantu Anda melakukan hal berikut:

- Lindungi data berharga dengan menerapkan jadwal pencadangan rutin.
- Mempertahankan cadangan sebagaimana diwajibkan oleh auditor atau kepatuhan internal.
- Mengurangi biaya penyimpanan dengan menghapus cadangan yang usang.

Menggunakan Amazon Data Lifecycle Manager, Anda dapat mengotomatiskan proses pengelolaan snapshot untuk instans EC2 (dan volume EBS terlampir) atau memisahkan volume EBS. Ini mendukung opsi seperti salinan lintas wilayah, sehingga Anda dapat menyalin snapshot secara otomatis ke Wilayah lain AWS . Menyalin snapshot ke Wilayah alternatif adalah salah satu pendekatan untuk mendukung upaya DR dan memulihkan opsi di Wilayah alternatif. Anda juga dapat menggunakan Amazon Data Lifecycle Manager untuk membuat kebijakan siklus hidup snapshot yang mendukung pemulihan snapshot cepat.

Amazon Data Lifecycle Manager adalah fitur yang disertakan dari Amazon EC2 dan Amazon EBS. Tidak ada biaya untuk Amazon Data Lifecycle Manager.

AWS Backup

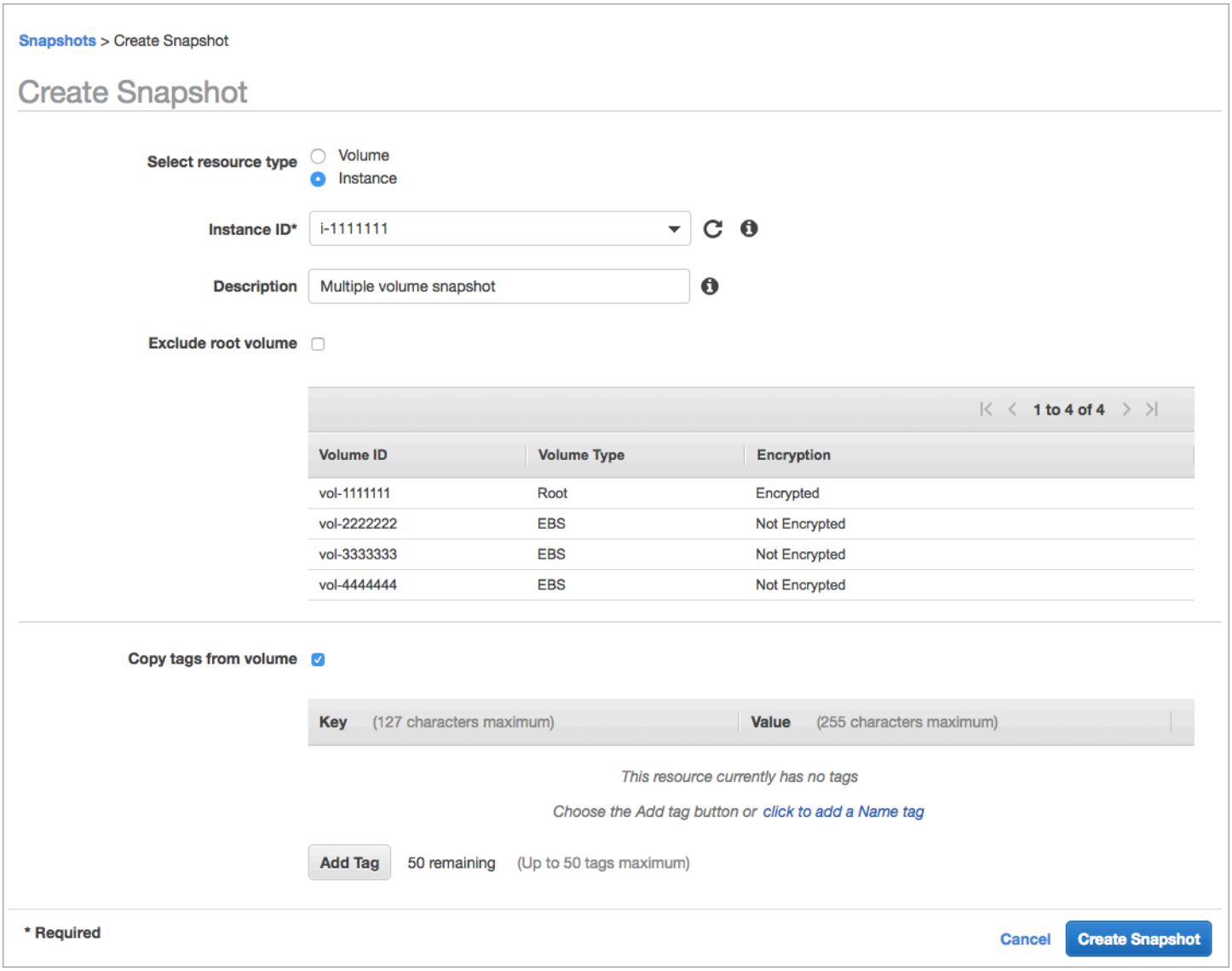
AWS Backup unik dari Amazon Data Lifecycle Manager karena Anda dapat membuat paket cadangan yang menyertakan sumber daya di beberapa layanan. AWS Anda dapat mengoordinasikan cadangan Anda untuk menutupi sumber daya yang Anda gunakan bersama daripada mengoordinasikan cadangan sumber daya secara individual.

AWS Backup juga mencakup konsep brankas cadangan, yang dapat membatasi akses ke titik pemulihan untuk cadangan Anda yang telah selesai. Operasi pemulihan dapat dimulai dari AWS Backup bukan melanjutkan ke setiap sumber daya individu dan memulihkan cadangan yang dibuat. AWS Backup juga mencakup sejumlah fitur tambahan, seperti manajemen audit dan pelaporan. Untuk informasi lebih lanjut, lihat Backup dan pemulihan menggunakanAWS Backup bagian panduan ini.

Melakukan backup multi-volume

Jika Anda ingin mencadangkan data pada volume EBS dalam array RAID menggunakan snapshot, snapshot harus konsisten. Ini karena snapshot volume ini dibuat secara independen. Memulihkan volume EBS dalam array RAID dari snapshot yang tidak sinkron menurunkan integritas array.

Untuk membuat kumpulan snapshot yang konsisten untuk array RAID Anda, gunakan operasi CreateSnapshotsAPI, atau masuk ke konsol Amazon EC2 dan pilih Elastic Block Store, Snapshots, Create Snapshot.



Snapshot instance yang memiliki beberapa volume yang dilampirkan dalam konfigurasi RAID diambil sebagai snapshot multi-volume, secara kolektif. Snapshot multi-volume menyediakan snapshot point-in-time, terkoordinasi data, dan konsisten crash di beberapa volume EBS yang dilampirkan ke instans EC2. Anda tidak perlu menghentikan instans Anda untuk berkoordinasi antar volume untuk mencapai konsistensi karena snapshot secara otomatis diambil di beberapa volume EBS. Setelah snapshot untuk volume dimulai (biasanya satu atau dua detik), sistem file dapat melanjutkan operasinya.

Setelah snapshot dibuat, setiap snapshot diperlakukan sebagai snapshot individu. Anda dapat melakukan semua operasi snapshot, seperti memulihkan, menghapus, dan Cross-region dan salinan akun, seperti yang Anda lakukan dengan snapshot volume tunggal. Anda juga dapat menandai snapshot multi-volume Anda seperti halnya snapshot volume tunggal. Kami menyarankan Anda

menandai snapshot multi-volume untuk mengelolanya secara kolektif selama pemulihan, penyalinan, atau penyimpanan. Untuk informasi selengkapnya, lihat dokumentasi AWS.

Anda juga dapat melakukan pencadangan ini dari manajer volume logis atau pencadangan tingkat sistem file. Dalam kasus ini, menggunakan agen cadangan tradisional memungkinkan data dicadangkan melalui jaringan. Sejumlah solusi cadangan berbasis agen tersedia di internet dan di. AWS Marketplace

Pendekatan alternatif adalah membuat replika volume sistem primer yang ada pada satu volume besar. Ini menyederhanakan proses pencadangan, karena hanya satu volume besar yang harus dicadangkan, dan pencadangan tidak terjadi pada sistem utama. Namun, pertama-tama tentukan apakah volume tunggal dapat bekerja cukup selama pencadangan dan apakah ukuran volume maksimum sesuai untuk aplikasi.

Melindungi cadangan Amazon EC2 Anda

Penting untuk mempertimbangkan keamanan cadangan Anda dan untuk mencegah penghapusan cadangan Anda secara tidak sengaja atau berbahaya. Anda dapat menggunakan sejumlah pendekatan secara kolektif untuk mencapai hal ini. Untuk mencegah hilangnya cadangan penting Anda karena pelanggaran keamanan, kami sarankan Anda menyalin cadangan Anda ke akun lain. AWS Jika Anda memiliki beberapa akun AWS, Anda dapat menetapkan akun terpisah sebagai akun arsip tempat semua akun lain dapat menyalin cadangan. Misalnya, Anda dapat melakukannya dengan cadangan lintas akun di. AWS Backup

Rencana pemulihan bencana Anda mungkin juga mengharuskan Anda untuk dapat mereproduksi instans EC2 di Wilayah AWS lain jika terjadi kegagalan regional. Anda dapat mendukung tujuan ini dengan menyalin cadangan Anda ke Wilayah lain dalam akun yang sama. Ini dapat memberikan lapisan tambahan perlindungan penghapusan yang tidak disengaja serta mendukung tujuan pemulihan bencana (DR). AWS Backup menyediakan dukungan untuk pencadangan lintas wilayah.

Pertimbangkan untuk memblokir izin IAM ke tindakan ec2: DeleteSnapshot dan ec2:. DeregisterImage Sebagai gantinya, Anda dapat mengizinkan kebijakan dan metode retensi mengelola siklus hidup snapshot EBS dan AMI Amazon EC2. Memblokir tindakan penghapusan adalah salah satu cara untuk menerapkan strategi write-once, read-many (WORM) untuk snapshot EBS Anda. Anda juga dapat menggunakan AWS Backup Vault Lock, yang menyediakan dukungan untuk snapshot EBS dan sumber daya lainnya. AWS

Selain itu, pertimbangkan untuk memblokir kemampuan pengguna untuk berbagi snapshot AMI dan EBS dengan memblokir tindakan EC2: ModifyImageAttribute dan ec2: IAM. ModifySnapshotAttribute

Ini akan mencegah AMI dan snapshot Anda dibagikan dengan AWS akun yang berada di luar organisasi Anda. Jika Anda menggunakan AWS Backup, batasi pengguna dari melakukan operasi serupa pada brankas cadangan. Untuk informasi lebih lanjut, lihat AWS Backup bagian panduan ini.

Amazon EC2 menyertakan fitur Recycle Bin yang dapat membantu Anda memulihkan snapshot EBS yang terhapus secara tidak sengaja. Jika Anda mengizinkan pengguna menghapus snapshot, aktifkan fitur ini agar snapshot yang diperlukan tidak dihapus secara permanen. Pengguna harus sangat berhati-hati dalam menghapus beberapa snapshot, karena konsol Amazon EC2 memungkinkan Anda memilih beberapa snapshot dan menghapusnya dalam satu operasi. Selain itu, berhati-hatilah saat Anda menggunakan skrip pembersihan dan otomatisasi sehingga Anda tidak sengaja menghapus snapshot yang Anda butuhkan. Fitur Recycle Bin membantu memberikan perlindungan dari jenis situasi ini.

Mengarsipkan snapshot EBS

Mengarsipkan snapshot EBS Anda bisa menjadi metode hemat biaya untuk menyimpan salinan volume untuk tujuan referensi yang tidak ingin Anda pulihkan selama 90 hari atau lebih. Ini bisa menjadi langkah perantara yang baik sebelum menghapus semua snapshot terkait secara permanen untuk volume EBS. Misalnya, Anda dapat mempertimbangkan pengarsipan snapshot sebagai end-of-lifecycle langkah untuk volume EBS yang tidak lagi digunakan. Pengarsipan daripada menghapus juga bisa menjadi metode retensi penghapusan yang lebih hemat biaya daripada menggunakan Recycle Bin.

Mengotomatiskan snapshot dan pembuatan AMI dengan Systems Manager, the AWS CLI, dan SDK AWS

Pendekatan pencadangan Anda mungkin memerlukan operasi sebelum dan sesudah snapshot atau AMI dibuat. Misalnya, Anda mungkin perlu menghentikan dan memulai layanan untuk menghentikan sistem file. Atau Anda mungkin perlu berhenti dan memulai instance Anda selama pembuatan AMI. Anda mungkin juga perlu membuat cadangan beberapa komponen dalam arsitektur Anda secara kolektif, masing-masing dengan langkah pra-pembuatan dan pasca-pembuatannya sendiri.

Anda dapat mengurangi waktu jendela pemeliharaan untuk pencadangan Anda dengan mengotomatiskan proses Anda dan memverifikasi bahwa proses pencadangan Anda diterapkan secara konsisten. Untuk mengotomatiskan operasi pra-pembuatan dan pasca-pembuatan kustom Anda, buat skrip proses pencadangan Anda dengan menggunakan AWS CLI dan SDK.

Otomatisasi Anda dapat didefinisikan dalam runbook Systems Manager yang dapat dijalankan sesuai permintaan atau selama jendela pemeliharaan Systems Manager. Anda dapat memberi

pengguna akses untuk menjalankan runbook Systems Manager tanpa perlu memberi mereka izin untuk perintah mengganggu Amazon EC2. Ini juga dapat membantu Anda memverifikasi bahwa proses pencadangan dan tag diterapkan secara konsisten oleh pengguna Anda. Anda dapat menggunakan CreateImage runbook AWS- CreateSnapshot dan AWS- untuk membuat snapshot dan AMI, atau Anda dapat memberikan izin kepada pengguna lain untuk menggunakannya. Systems Manager juga menyertakan UpdateWindowsAmi runbook AWS- UpdateLinuxAmi dan AWS- untuk mengotomatiskan patching AMI dan pembuatan AMI.

Anda juga dapat menggunakan AWS CLI dan AWS Tools for Windows PowerShelluntuk mengotomatiskan snapshot dan proses pembuatan AMI Anda. Anda dapat menggunakan AWS CLI perintah aws ec2 create-snapshot untuk membuat snapshot volume EBS sebagai satu langkah dalam otomatisasi Anda. Anda dapat menggunakan perintah aws ec2 create-snapshots untuk membuat snapshot tersinkronisasi yang konsisten dengan crash dari semua volume yang dilampirkan ke instans EC2 Anda.

Anda dapat menggunakan AWS CLI untuk membuat AMI baru. Anda dapat menggunakan perintah aws ec2 register-image untuk membuat gambar baru untuk instans EC2 Anda. Untuk mengotomatiskan shutdown, pembuatan gambar, dan restart instance Anda, gabungkan perintah ini dengan perintah aws ec2 stop-instance dan aws ec2 start-instances.

Memulihkan volume Amazon EBS atau instans EC2

Jika Anda hanya perlu mengembalikan satu volume yang terpasang pada instans EC2, Anda dapat mengembalikan volume tersebut secara terpisah, melepaskan volume yang ada, dan melampirkan volume yang dipulihkan ke instans EC2 Anda. Jika Anda perlu memulihkan seluruh instans EC2, termasuk semua volume yang terkait, Anda harus menggunakan cadangan Amazon Machine Image (AMI) dari instans Anda.

Untuk mengurangi waktu pemulihan dan dampak pada aplikasi dan proses yang bergantung, proses pemulihan Anda harus mempertimbangkan sumber daya yang digantikannya. Untuk hasil terbaik, uji proses pemulihan Anda secara teratur di lingkungan yang lebih rendah (misalnya, non-produksi) untuk memverifikasi bahwa proses Anda memenuhi tujuan titik pemulihan (RPO) dan tujuan waktu pemulihan (RTO) dan bahwa proses pemulihan berfungsi seperti yang diharapkan. Pertimbangkan bagaimana proses pemulihan akan memengaruhi aplikasi dan layanan yang bergantung pada contoh yang Anda pulihkan, dan kemudian koordinasikan pemulihan seperlunya. Cobalah untuk mengotomatisasi dan menguji proses pemulihan sebanyak mungkin untuk mengurangi risiko proses pemulihan Anda gagal atau diimplementasikan secara tidak konsisten.

Jika Anda menggunakan Elastic Load Balancing, dengan beberapa instans yang melayani lalu lintas, Anda dapat menghilangkan instans yang gagal atau terganggu. Kemudian Anda dapat memulihkan instance baru untuk menggantinya sementara instance lain terus melayani lalu lintas tanpa gangguan kepada pengguna.

Proses pemulihan berikut yang dijelaskan adalah untuk contoh yang tidak menggunakan Elastic Load Balancing:

- Memulihkan file dan direktori individual dari snapshot EBS
- Memulihkan volume EBS dari snapshot Amazon EBS
- Membuat atau memulihkan instans EC2 dari snapshot EBS
- Memulihkan instance yang sedang berjalan dari AMI

Memulihkan file dan direktori dari snapshot EBS

Snapshot EBS memberikan replika point-in-time yang tepat dari volume asli yang digunakan untuk membuat snapshot. Untuk mengembalikan file atau direktori individual, Anda harus melakukan hal berikut:

1. Pertama, kembalikan volume dari snapshot EBS yang berisi file atau direktori.
2. Lampirkan volume ke instans EC2 yang ingin Anda pulihkan file.
3. Salin file dari volume yang dipulihkan ke volume instans EC2 Anda.
4. Lepaskan dan hapus volume yang dipulihkan.

Memulihkan volume EBS dari snapshot Amazon EBS

Anda dapat memulihkan volume yang dilampirkan ke instans EC2 yang ada dengan membuat volume dari snapshot dan melampirkannya ke instans Anda. Anda dapat menggunakan konsol, operasi AWS CLI, atau API untuk membuat volume dari snapshot yang ada. Anda kemudian dapat memasang volume ke instance dengan menggunakan sistem operasi.

Perhatikan bahwa data dari snapshot Amazon EBS dimuat secara asinkron ke dalam volume EBS. Jika aplikasi mengakses volume di mana data tidak dimuat, ada latensi yang lebih tinggi dari biasanya saat data dimuat dari Amazon S3. Untuk menghindari dampak ini untuk aplikasi yang sensitif terhadap latensi, Anda memiliki dua opsi:

- Anda dapat menginisialisasi volume EBS.
- Dengan biaya tambahan, Amazon EBS mendukung pemulihan snapshot cepat, yang menghilangkan kebutuhan inisialisasi volume Anda.

Jika Anda mengganti volume yang harus menggunakan titik pemasangan yang sama, lepaskan volume itu sehingga Anda dapat memasang volume baru di tempatnya. Untuk melepas volume, pertama-tama hentikan proses apa pun yang menggunakan volume. Jika Anda mengganti volume root, Anda harus menghentikan instance terlebih dahulu sebelum Anda dapat melepaskan volume root.

Misalnya, ikuti langkah-langkah berikut untuk mengembalikan volume ke point-in-time cadangan sebelumnya dengan menggunakan konsol:

1. Di konsol Amazon EC2, pada menu Elastic Block Store, pilih Snapshots.
2. Cari snapshot yang ingin Anda pulihkan, dan pilih.
3. Pilih Tindakan, lalu pilih Buat Volume.
4. Buat volume baru di Availability Zone yang sama dengan instans EC2 Anda.
5. Di konsol Amazon EC2, pilih instans.
6. Dalam detail instance, catat nama perangkat yang ingin Anda ganti di entri perangkat Root atau entri Blokir Perangkat.
7. Pasang volumenya. Prosesnya berbeda untuk volume root dan volume non-root.

   Untuk volume root:

   a. Hentikan instans EC2.
   b. Pada menu EC2 Elastic Block Store Volumes, pilih volume root yang ingin Anda ganti.
   c. Pilih Tindakan, lalu pilih Lepaskan Volume.
   d. Pada menu EC2 Elastic Block Store Volumes, pilih volume baru.
   e. Pilih Tindakan, lalu pilih Lampirkan Volume.
   f. Pilih instance yang ingin Anda lampirkan volumenya, dan gunakan nama perangkat yang sama dengan yang Anda catat sebelumnya.

   Untuk volume non-root:

   a. Pada menu EC2 Elastic Block Store Volumes, pilih volume non-root yang ingin Anda ganti.
   b. Pilih Tindakan, lalu pilih Lepaskan Volume.

c. Pasang volume baru dengan memilihnya di menu EC2 Elastic Block Store Volumes dan kemudian pilih Actions, Attach Volume. Pilih instance yang ingin Anda lampirkan, lalu pilih nama perangkat yang tersedia.

d. Menggunakan sistem operasi misalnya, lepaskan volume yang ada, dan kemudian pasang volume baru di tempatnya.

   Di Linux, Anda dapat menggunakan `umount` perintah. Di Windows, Anda dapat menggunakan manajer volume logis (LVM) seperti utilitas sistem Manajemen Disk.

e. Lepaskan volume sebelumnya yang mungkin Anda ganti dengan memilihnya di menu Volume Toko Blok Elastis EC2 dan kemudian pilih Tindakan, Lepaskan Volume.

Anda juga dapat menggunakan kombinasi AWS CLI dengan perintah sistem operasi untuk mengotomatiskan langkah-langkah ini.

Membuat atau memulihkan instans EC2 dari snapshot EBS

Untuk membuat cadangan yang akan digunakan untuk memulihkan seluruh instans EC2, sebaiknya buat Amazon Machine Image (AMI). AMI menangkap informasi mesin seperti jenis virtualisasi. Mereka juga membuat snapshot untuk setiap volume yang dilampirkan ke instans EC2, termasuk pemetaan perangkat mereka, sehingga mereka dapat dipulihkan dalam konfigurasi yang sama.

Namun, jika Anda harus menggunakan snapshot EBS untuk memulihkan instance, pertama-tama buat AMI dari snapshot EBS yang akan menjadi volume root untuk instans EC2 baru Anda:

1. Di konsol Amazon EC2, pada menu Elastic Block Store, pilih Snapshots.
2. Cari snapshot yang akan digunakan untuk membuat volume root untuk instans EC2 baru Anda, dan pilih.
3. Pilih Tindakan, lalu pilih Buat Gambar dari Snapshot.
4. Masukkan nama untuk gambar Anda (misalnya,`YYYYMMDD-restore-for-i-012345678998765de`), dan pilih opsi yang sesuai untuk gambar baru Anda.

Setelah gambar dibuat dan tersedia, Anda dapat meluncurkan instans EC2 baru yang akan menggunakan snapshot EBS untuk volume root.

Memulihkan instance yang sedang berjalan dari AMI

Anda dapat memunculkan instance baru dari cadangan AMI untuk mengganti instance yang sudah berjalan. Salah satu pendekatannya adalah menghentikan instans yang ada, menjaganya tetap offline saat Anda meluncurkan instance baru dari AMI Anda, dan melakukan pembaruan yang diperlukan. Pendekatan ini mengurangi risiko konflik dari kedua contoh yang berjalan secara bersamaan. Ini adalah pendekatan yang dapat diterima jika layanan yang disediakan instans Anda sedang down atau Anda melakukan pemulihan selama jendela pemeliharaan. Setelah menguji instans baru, Anda dapat menetapkan kembali alamat IP Elastis yang dialokasikan ke instans lama. Kemudian Anda dapat memperbarui catatan Layanan Nama Domain (DNS) apa pun untuk menunjuk ke instance baru.

Namun, jika selama pemulihan Anda harus meminimalkan waktu henti instans dalam layanan Anda, pertimbangkan untuk meluncurkan dan menguji instance baru dari cadangan AMI Anda. Kemudian ganti instance yang ada dengan instance baru.

Saat kedua instance berjalan, Anda harus mencegah instans baru menyebabkan tabrakan tingkat platform atau tingkat aplikasi. Misalnya, Anda mungkin mengalami masalah dengan instance Windows yang bergabung dengan domain yang berjalan dengan SID dan nama komputer yang sama. Anda mungkin mengalami masalah serupa dengan aplikasi dan layanan jaringan yang memerlukan pengidentifikasi unik.

Untuk mencegah server dan layanan lain terhubung ke instans baru Anda sebelum siap, gunakan grup keamanan untuk memblokir sementara semua koneksi masuk untuk instance baru Anda kecuali untuk alamat IP Anda sendiri untuk akses dan pengujian. Anda juga dapat memblokir koneksi keluar sementara untuk instance baru untuk mencegah layanan dan aplikasi memulai koneksi atau pembaruan apa pun ke sumber daya lain. Ketika instance baru siap, hentikan instance yang ada, mulai layanan dan proses pada instance baru, lalu buka blokir koneksi jaringan masuk atau keluar yang Anda terapkan.

Backup dan pemulihan dari infrastruktur lokal ke AWS

Anda dapat menggunakan AWS penyimpanan cadangan infrastruktur lokal yang tahan lama dan di luar lokasi Anda. Dengan menggunakan layanan AWS penyimpanan dalam skenario ini, Anda dapat fokus pada tugas pencadangan dan pengarsipan. Anda tidak perlu khawatir tentang penyediaan infrastruktur penyimpanan, penskalaan, atau kapasitas infrastruktur untuk tugas pencadangan Anda.

Amazon S3 menyediakan operasi API dan SDK yang ekstensif untuk diintegrasikan ke dalam pendekatan pencadangan dan pemulihan baru dan yang sudah ada. Ini juga memberi vendor perangkat lunak cadangan cara untuk secara langsung mengintegrasikan aplikasi mereka dengan solusi AWS penyimpanan.

Dalam skenario ini, backup dan arsip perangkat lunak yang Anda gunakan di infrastruktur lokal langsung berinteraksi dengan AWS melalui operasi API. Karena perangkat lunak pencadangan AWS-aware, ia mencadangkan data dari server lokal langsung ke Amazon S3.

Jika perangkat lunak cadangan yang ada tidak mendukung AWS Cloud secara native, Anda dapat menggunakan Storage Gateway. Layanan penyimpanan cloud, Storage Gateway memberi sistem lokal Anda akses ke penyimpanan cloud yang dapat diskalakan. Ini mendukung protokol penyimpanan standar terbuka yang bekerja dengan aplikasi yang ada sambil menyimpan data Anda yang dienkripsi dengan aman di Amazon S3. Anda dapat menggunakan Storage Gateway sebagai bagian dari pendekatan pencadangan dan pemulihan untuk beban kerja penyimpanan berbasis blok lokal.

Storage Gateway sangat membantu dalam skenario hybrid di mana Anda ingin beralih ke penyimpanan berbasis cloud untuk backup Anda. Storage Gateway juga membantu Anda mengurangi investasi modal di penyimpanan lokal. Anda menggunakan Storage Gateway sebagai VM atau perangkat keras khusus. Panduan ini berfokus pada bagaimana Storage Gateway berlaku untuk pencadangan dan pemulihan.

Storage Gateway menyediakan tiga opsi berbeda untuk memenuhi persyaratan yang berbeda:

- Gateway file untuk menyimpan file data aplikasi dan gambar cadangan sebagai objek tahan lama di penyimpanan cloud Amazon S3 menggunakan akses berbasis SMB atau berbasis NFS.
- Gerbang volume untuk menyajikan volume penyimpanan blok iSCSI berbasis cloud ke aplikasi lokal Anda. Gerbang volume menyediakan cache lokal atau volume penuh di tempat sambil juga menyimpan salinan lengkap volume Anda di AWS Cloud.

- Gateway tape untuk mengarahkan perangkat lunak cadangan tepercaya ke gateway penyimpanan lokal yang, pada gilirannya, terhubung ke Amazon S3. Opsi ini memberikan skala dan daya tahan cloud untuk retensi jangka panjang yang aman tanpa mengganggu investasi atau proses yang ada.

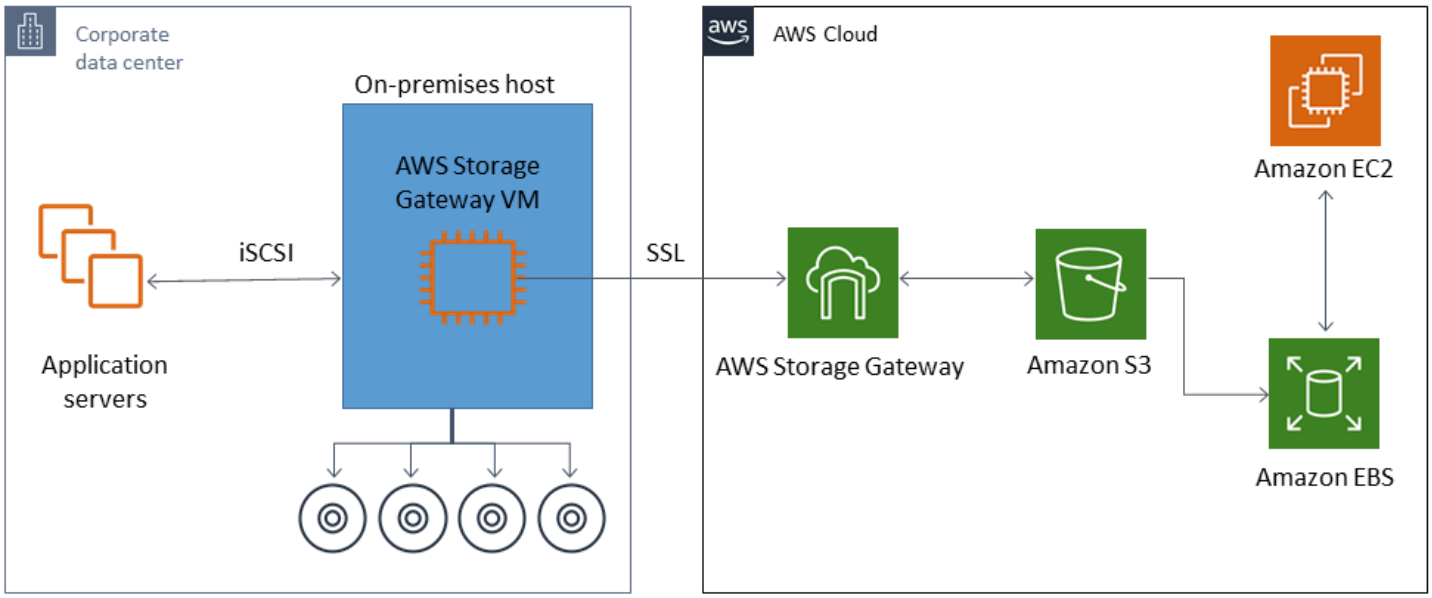
Gerbang file

Banyak organisasi memulai perjalanan cloud mereka dengan memindahkan data sekunder dan tersier, seperti backup, ke cloud. Dukungan antarmuka SMB dan NFS gateway file menyediakan cara bagi grup TI untuk mentransisikan pekerjaan pencadangan dari sistem cadangan lokal yang ada ke cloud. Aplikasi backup, alat database asli, atau skrip yang dapat menulis ke SMB atau NFS dapat menulis ke gateway file. Gateway file menyimpan cadangan sebagai objek Amazon S3 berukuran hingga 5 TiB. Dengan cache lokal berukuran cukup, cadangan terbaru dapat digunakan untuk pemulihan di tempat yang cepat. Kebutuhan retensi jangka panjang ditangani dengan meningkatkan cadangan ke kelas penyimpanan S3 Standard-Infrequent Access dan S3 Glacier berbiaya rendah.

File gateway menyediakan jalan aktif untuk penyimpanan berbasis blok Anda ke Amazon S3 untuk pencadangan di luar situs yang sangat tahan lama. Ini sangat berguna untuk skenario di mana file yang baru-baru ini dicadangkan harus dipulihkan dengan cepat. Karena gateway file mendukung protokol SMB dan NFS, pengguna dapat mengakses file dengan cara yang sama mereka akan mengakses berbagi file jaringan. Anda juga dapat memanfaatkan kemampuan pembuatan versi objek Amazon S3. Menggunakan versi objek, Anda dapat memulihkan versi objek sebelumnya untuk file dan kemudian dengan mudah mengaksesnya dengan menggunakan SMB atau NFS.

Gerbang volume

Gerbang volume memungkinkan Anda menyediakan volume penyimpanan blok iSCSI berbasis Internet untuk server lokal. Gerbang volume menyimpan data volume Anda ke Amazon S3 untuk penyimpanan offsite berbasis cloud yang tahan lama dan dapat diskalakan. Gerbang volume memfasilitasi pengambilan point-in-time snapshot penuh volume Anda dan menyimpannya di cloud sebagai snapshot Amazon EBS. Setelah disimpan sebagai snapshot, seluruh volume dapat dipulihkan sebagai volume EBS dan dilampirkan ke instans EC2, mempercepat solusi DR berbasis cloud. Volume juga dapat dikembalikan ke Storage Gateway, memungkinkan aplikasi lokal Anda kembali ke status sebelumnya.



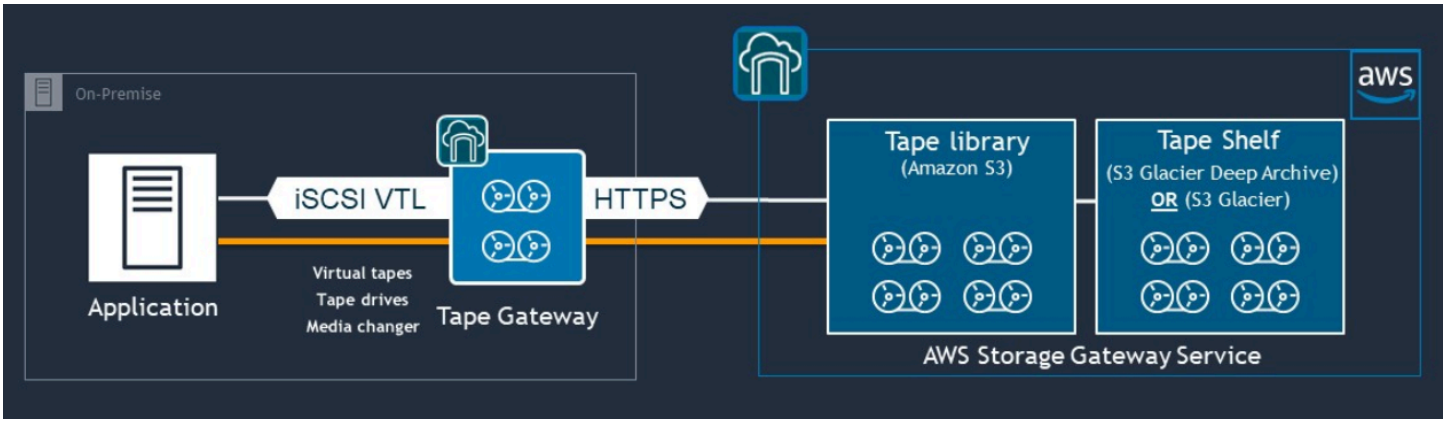
Karena gateway volume terintegrasi dengan fitur volume Amazon EBS Amazon EC2, Anda dapat AWS Backup menggunakannya untuk mengotomatiskan dan menjadwalkan proses snapshot Anda. Gerbang volume memberi Anda manfaat tambahan dari snapshot Amazon EBS dan fitur penandaan Amazon S3 yang tahan lama dan didukung Amazon S3. Untuk informasi selengkapnya, lihat dokumentasi snapshot Amazon EBS.

Gerbang pita

Gateway tape menawarkan daya tahan tinggi, penyimpanan berjenjang berbiaya rendah, dan fitur ekstensif Amazon S3 untuk toko cadangan pita virtual di luar lokasi Anda. Semua kaset virtual Anda yang disimpan di Amazon S3 direplikasi dan disimpan di setidaknya tiga Availability Zone yang tersebar secara geografis. Kaset virtual Anda dilindungi oleh 11 sembilan daya tahan.

AWS juga melakukan pemeriksaan fixity secara teratur untuk mengonfirmasi bahwa data Anda dapat dibaca dan tidak ada kesalahan yang diperkenalkan. Semua kaset yang disimpan di Amazon S3 dilindungi oleh enkripsi sisi server menggunakan kunci default atau kunci Anda. AWS KMS Selain itu, Anda menghindari risiko keamanan fisik yang terkait dengan portabilitas pita. Dengan gateway tape, Anda mendapatkan data yang benar, dibandingkan dengan pergudangan kaset di luar lokasi, di mana Anda mungkin menerima pita yang salah atau rusak selama pemulihan.

Anda dapat menghemat biaya penyimpanan bulanan saat menyimpan data Anda di Amazon S3. Anda dapat menyimpan lebih banyak lagi untuk kebutuhan arsip jangka panjang Anda dengan menggunakan S3 Glacier Deep Archive.



Gateway tape bertindak sebagai pustaka pita virtual (VTL) yang membentang dari lingkungan lokal Anda hingga layanan penyimpanan yang sangat skalabel, redundan, dan tahan lama: Amazon S3, Pengambilan Fleksibel Gletser S3, dan Arsip Dalam Gletser S3.

Gateway tape menyajikan Storage Gateway ke aplikasi cadangan Anda yang ada sebagai VTL berbasis iSCSI standar terbuka, dengan pengubah media virtual dan drive tape virtual. Anda dapat terus menggunakan aplikasi cadangan dan alur kerja yang ada saat menulis ke kumpulan kaset virtual yang disimpan di Amazon S3 yang dapat diskalakan secara besar-besaran. Ketika Anda tidak lagi memerlukan akses langsung atau sering ke data pada pita virtual, aplikasi cadangan Anda dapat mengarsipkannya ke dalam S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive, yang selanjutnya mengurangi biaya penyimpanan.

Anda dapat mengambil rekaman yang diarsipkan dalam S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive biasanya masing-masing dalam 3-5 jam atau 12 jam. Gateway tape dapat digunakan dengan aplikasi cadangan yang kompatibel dengan antarmuka perpustakaan tape berbasis iSCSI untuk mengakses kaset virtual. Juga pertimbangkan ukuran penyimpanan minimum 100-GB per kaset. Untuk informasi lebih lanjut, tinjau daftar aplikasi cadangan pihak ketiga yang mendukung gateway tape.

Backup dan pemulihan aplikasi dariAWSke pusat data Anda

Anda mungkin memiliki kebijakan yang mengharuskan Anda menerapkan skenario seperti DR atau kelangsungan bisnis untuk beban kerja berbasis Internet dan infrastruktur lokal Anda. Jika Anda sudah memiliki kerangka kerja cadangan data untuk server lokal, Anda dapat memperpanjangnya keAWSsumber daya melalui koneksi VPN atau melaluiAWS Direct Connect. Anda dapat menginstal agen cadangan pada instans EC2 dan mencadangkan data dan aplikasi Anda sesuai dengan kebijakan perlindungan data Anda. Anda juga dapat menggunakan Amazon S3 sebagai layanan perantara untuk menyimpan cadangan tingkat aplikasi Anda. Anda kemudian dapat menggunakan operasi API, SDK, atauAWS CLIuntuk memulihkan data ke lingkungan lokal Anda.

Untuk mencadangkan data diAWSlayanan selain Amazon EC2, menggunakanAWS CLI, SDK, dan operasi API untuk mengekstrak data ke dalam format yang Anda inginkan. Kemudian salin data ke Amazon S3, dan salin dari Amazon S3 ke lingkungan lokal Anda. Beberapa layanan menyediakan ekspor langsung ke Amazon S3. Misalnya, Amazon RDS mendukungcadangan aslidatabase Microsoft SQL Server ke Amazon S3.

Backup dan pemulihanAWS layanan cloud-native

Pendekatan pencadangan dan pemulihan Anda harus mencakupAWS layanan yang digunakan dalam beban kerja Anda. AWSmenyediakan fitur dan opsi khusus layanan untuk mengelola dan berinteraksi dengan data Anda. Anda dapat menggunakan operasi konsol, SDKAWS CLI, dan API untuk mengimplementasikan pencadangan dan pemulihan untukAWS layanan yang Anda gunakan. Panduan ini mencakup Amazon RDS dan Amazon DynamoDB sebagai contoh. AWS Backupmendukung DynamoDB dan Amazon RDS dan harus digunakan jika memenuhi kebutuhan Anda.

Backup dan pemulihan untuk Amazon RDS

Amazon RDS menyertakan fitur untuk mengotomatiskan pencadangan database. Amazon RDS menciptakan snapshot volume penyimpanan instans basis data Anda, mencadangkan seluruh instans DB, bukan basis data individu. Dengan menggunakan Amazon RDS, Anda dapat membuat jendela cadangan untuk pencadangan otomatis, membuat snapshot instans database, dan berbagi dan menyalin snapshot di seluruh Wilayah dan akun.

Amazon RDS menyediakan dua opsi berbeda untuk mencadangkan dan memulihkan instans DB Anda:

- Pencadangan otomatis menyediakan point-in-time pemulihan (PITR) instans DB Anda. Backup diaktifkan secara default saat Anda membuat instans DB.

  Amazon RDS melakukan pencadangan harian penuh data Anda selama jendela cadangan yang Anda tentukan saat Anda membuat instans DB. Anda dapat mengonfigurasi periode penyimpanan hingga 35 hari untuk pencadangan otomatis. Amazon RDS juga mengunggah log transaksi untuk instans DB ke Amazon S3 setiap 5 menit. Amazon RDS menggunakan cadangan harian Anda bersama dengan log transaksi database Anda untuk memulihkan instans DB Anda. Anda dapat memulihkan instans ke detik berapa pun selama periode retensi, hingga`LatestRestorableTime` (biasanya, lima menit terakhir).

  Untuk menemukan waktu pemulihan terbaru untuk instans DB Anda, gunakan panggilan`DescribeDBInstances` API. Atau lihat tab Deskripsi untuk database di konsol Amazon RDS.

  Saat Anda memulai PITR, log transaksi digabungkan dengan cadangan harian yang paling tepat untuk memulihkan instans DB Anda ke waktu yang diminta.

- Snapshot DB adalah pencadangan yang dapat Anda gunakan untuk memulihkan instans DB Anda ke status yang diketahui sesering yang Anda suka. Anda kemudian dapat mengembalikan ke keadaan itu kapan saja. Anda dapat menggunakan konsol Amazon RDS atau panggilan`CreateDBSnapshot` API untuk membuat snapshot DB. Snapshot ini disimpan sampai Anda menggunakan konsol atau panggilan`DeleteDBSnapshot` API untuk menghapusnya secara eksplisit.

Kedua opsi cadangan ini didukung untuk Amazon RDS diAWS Backup, yang juga menyediakan fitur lainnya. PertimbangkanAWS Backup untuk menggunakan untuk menyiapkan paket cadangan standar untuk database Amazon RDS Anda, dan gunakan opsi pencadangan instans yang dimulai pengguna saat rencana cadangan untuk database tertentu bersifat unik.

Amazon RDS mencegah akses langsung ke penyimpanan dasar yang digunakan oleh instans DB. Ini juga mencegah Anda mengekspor database secara langsung pada instans DB RDS ke disk lokalnya. Dalam beberapa kasus, Anda dapat menggunakan fungsi backup dan restore asli menggunakan utilitas klien. Misalnya, Anda dapat menggunakan perintah mysqldump dengan database MySQL Amazon RDS untuk mengekspor database ke mesin klien lokal Anda. Dalam beberapa kasus, Amazon RDS juga menyediakan opsi tambahan untuk melakukan pencadangan asli dan pemulihan database. Misalnya, Amazon RDS menyediakan prosedur tersimpan untuk mengekspor dan mengimpor cadangan database RDS dari database SQL Server.

Pastikan untuk menguji proses pemulihan database Anda secara menyeluruh dan dampaknya terhadap klien database sebagai bagian dari pendekatan pencadangan dan pemulihan keseluruhan Anda.

Menggunakan data DNS CNAME untuk mengurangi dampak klien selama pemulihan database

Saat Anda memulihkan database dengan menggunakan snapshot instans PITR atau DB RDS, instans DB baru dengan titik akhir baru akan dibuat. Dengan cara ini, Anda dapat membuat beberapa instans DB dari snapshot DB tertentu atau titik waktu. Ada pertimbangan khusus saat Anda memulihkan instans DB RDS untuk mengganti instans DB RDS langsung. Misalnya, Anda harus menentukan bagaimana Anda akan mengarahkan klien database yang ada ke instance baru dengan gangguan dan modifikasi minimal. Anda juga harus memastikan kontinuitas dan konsistensi dalam data dalam database dengan mempertimbangkan waktu data yang dipulihkan dan waktu pemulihan ketika instance baru mulai menerima penulisan.

Anda dapat membuat data DNS CNAME terpisah yang mengarah ke titik akhir instans DB Anda dan meminta klien Anda menggunakan nama DNS ini. Kemudian Anda dapat memperbarui CNAME untuk menunjuk ke titik akhir baru yang dipulihkan tanpa harus memperbarui klien database Anda.

Atur Time to Live (TTL) untuk catatan CNAME Anda ke nilai yang sesuai. TTL yang Anda tentukan menentukan berapa lama rekaman di-cache dengan resolver DNS sebelum permintaan lain dibuat. Penting untuk dicatat bahwa beberapa resolver atau aplikasi DNS mungkin tidak menghormati TTL, dan mereka mungkin menyimpan catatan lebih lama dari TTL. Untuk Amazon Route 53, jika Anda menentukan nilai yang lebih lama (misalnya, 172.800 detik, atau dua hari), Anda mengurangi jumlah panggilan yang harus dilakukan oleh resolver rekursif DNS ke Route 53 untuk mendapatkan informasi terbaru dalam catatan ini. Ini mengurangi latensi dan mengurangi tagihan Anda untuk layanan Route 53. Untuk informasi lebih lanjut, lihat Cara Amazon Route 53 merutekan lalu lintas untuk domain Anda.

Aplikasi dan sistem operasi klien mungkin juga menyimpan informasi DNS yang harus Anda siram atau restart untuk memulai permintaan resolusi DNS baru dan mengambil catatan CNAME yang diperbarui.

Saat Anda memulai pemulihan database dan mengalihkan lalu lintas ke instans yang dipulihkan, verifikasi bahwa semua klien Anda menulis ke instans yang dipulihkan, bukan instans sebelumnya. Arsitektur data Anda mungkin mendukung pemulihan database Anda, memperbarui DNS untuk mengalihkan lalu lintas ke instans yang dipulihkan, dan kemudian memulihkan data apa pun yang mungkin masih ditulis ke instans sebelumnya. Jika ini bukan masalahnya, Anda dapat menghentikan instans yang ada sebelum memperbarui data DNS CNAME. Maka semua akses berasal dari instance Anda yang baru dipulihkan. Ini untuk sementara dapat menyebabkan masalah koneksi untuk beberapa klien database Anda yang dapat Anda tangani secara individual. Untuk mengurangi dampak klien, Anda dapat melakukan pemulihan database selama jendela pemeliharaan.

Tulis aplikasi Anda untuk menangani kegagalan koneksi database dengan anggun dengan percobaan ulang menggunakan backoff eksponensial. Hal ini memungkinkan aplikasi Anda untuk pulih ketika koneksi database menjadi tidak tersedia selama pemulihan tanpa menyebabkan aplikasi Anda tiba-tiba mogok.

Setelah menyelesaikan proses pemulihan, Anda dapat menyimpan instans sebelumnya dalam keadaan berhenti. Atau Anda dapat menggunakan aturan grup keamanan untuk membatasi lalu lintas ke instans sebelumnya sampai Anda puas bahwa itu tidak lagi diperlukan. Untuk pendekatan penonaktifan bertahap, pertama-tama batasi akses ke database yang berjalan oleh grup keamanan. Anda akhirnya dapat menghentikan instans saat tidak lagi diperlukan. Akhirnya, ambil snapshot instans basis data dan hapus.

Backup dan pemulihan untuk DynamoDB

DynamoDB menyediakan PITR, yang membuat pencadangan data tabel DynamoDB Anda. Bila diaktifkan, DynamoDB mempertahankan pencadangan tambahan tabel selama 35 hari sampai Anda secara eksplisit mematikannya.

Anda juga dapat membuat cadangan sesuai permintaan dari tabel DynamoDB Anda dengan menggunakan konsol DynamoDB,AWS CLI, atau DynamoDB API. Untuk informasi lebih lanjut, lihat Mencadangkan tabel DynamoDB. Anda dapat menjadwalkan pencadangan berkala atau future dengan menggunakanAWS Backup, atau Anda dapat menyesuaikan dan mengotomatiskan pendekatan pencadangan Anda dengan menggunakan fungsi Lambda. Untuk informasi selengkapnya tentang penggunaan fungsi Lambda untuk Backup DynamoDB, lihat posting blog Solusi nirkabel untuk menjadwalkan Pencadangan Sesuai Permintaan Amazon DynamoDB Anda. Jika Anda tidak ingin membuat penjadwalan skrip dan pekerjaan pembersihan, Anda dapat menggunakanAWS Backup untuk membuat rencana pencadangan. Paket cadangan mencakup jadwal dan kebijakan penyimpanan untuk tabel DynamoDB Anda. AWS Backupmembuat cadangan dan menghapus cadangan sebelumnya berdasarkan jadwal retensi Anda. AWS Backupjuga mencakup opsi cadangan DynamoDB tingkat lanjut yang tidak tersedia di layanan DynamoDB, termasuk penyimpanan bertingkat dengan biaya lebih rendah, dan salinan lintas akun dan lintas wilayah. Untuk informasi lebih lanjut, lihat Pencadangan DynamoDB.

Anda harus secara manual mengatur berikut ini pada tabel DynamoDB:

- Kebijakan penskalaan
- Kebijakan IAM
- CloudWatch Metrik dan alarm
- Tanda
- Pengaturan stream
- Pengaturan

Anda dapat memulihkan hanya seluruh data tabel ke tabel baru dari pencadangan. Anda dapat menulis ke tabel yang dipulihkan hanya setelah menjadi aktif.

Proses pemulihan Anda harus mempertimbangkan bagaimana klien akan diarahkan untuk menggunakan nama tabel yang baru dipulihkan. Anda dapat mengonfigurasi aplikasi dan klien Anda untuk mengambil nama tabel DynamoDB dari file konfigurasi, nilaiAWS Systems Manager Parameter

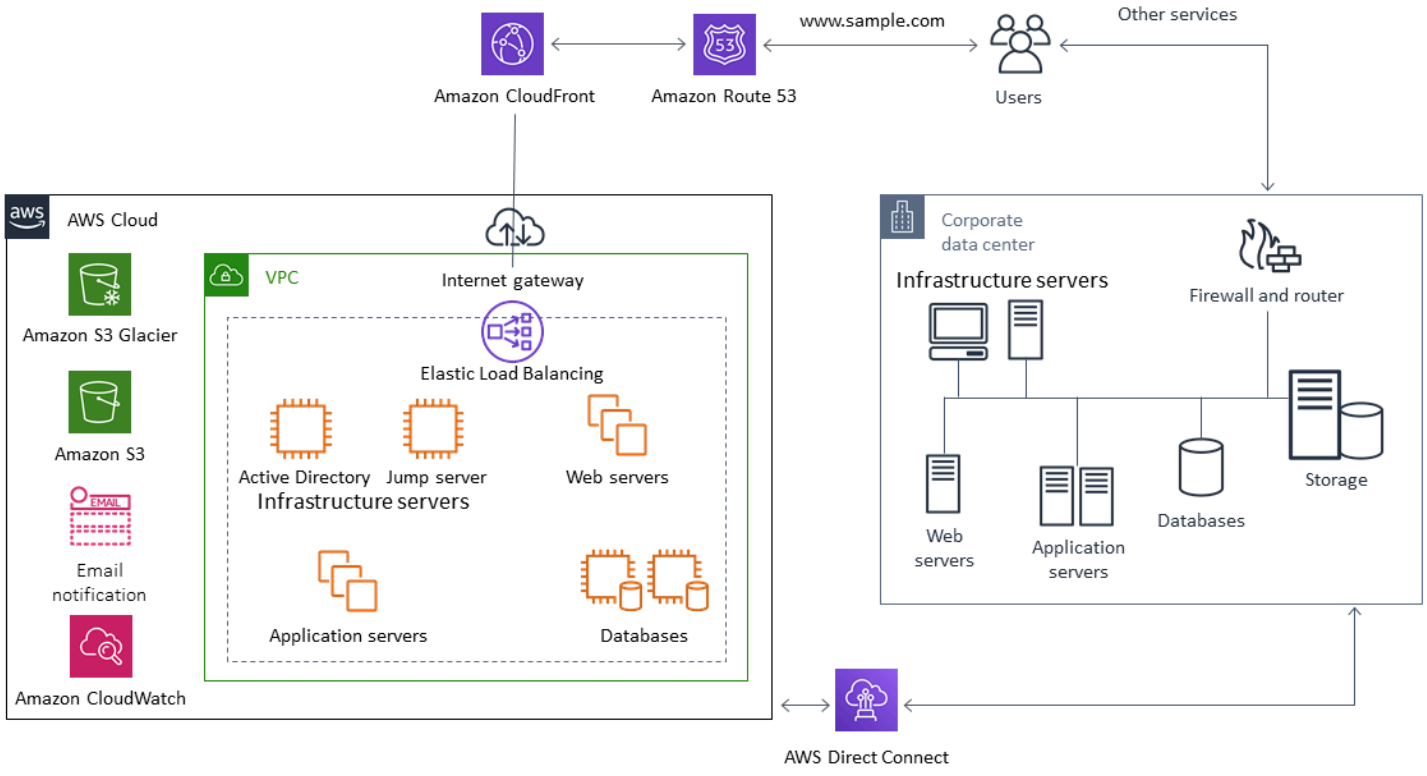
Store, atau referensi lain yang dapat diperbarui secara dinamis untuk mencerminkan nama tabel yang harus digunakan klien.

Sebagai bagian dari proses pemulihan, Anda harus mempertimbangkan dengan cermat proses peralihan Anda. Anda dapat memilih untuk menolak akses ke tabel DynamoDB yang ada melalui izin IAM dan memungkinkan akses ke tabel baru Anda. Anda kemudian dapat memperbarui konfigurasi aplikasi dan klien untuk menggunakan tabel baru. Anda mungkin juga perlu merekonsiliasi perbedaan antara tabel DynamoDB yang ada dan tabel DynamoDB yang baru dipulihkan.

Backup dan recovery untuk arsitektur hybrid

Penerapan cloud-native dan lokal yang dibahas dalam panduan ini dapat digabungkan ke dalam skenario hibrid di mana lingkungan beban kerja memiliki komponen lokal dan infrastruktur. AWS Sumber daya, termasuk server web, server aplikasi, server pemantauan, database, dan Microsoft Active Directory, di-host baik di pusat data pelanggan atau di AWS. Aplikasi yang berjalan di AWS Cloud terhubung ke aplikasi yang berjalan di tempat.

Ini menjadi skenario umum untuk beban kerja perusahaan. Banyak perusahaan memiliki pusat data mereka sendiri dan digunakan AWS untuk menambah kapasitas. Pusat data pelanggan ini sering terhubung ke AWS jaringan dengan tautan jaringan berkapasitas tinggi. Misalnya, dengan AWS Direct Connect, Anda dapat membuat konektivitas pribadi dan khusus dari pusat data lokal ke AWS. Ini memberikan bandwidth dan latensi yang konsisten untuk mengunggah data ke cloud untuk tujuan perlindungan data. Ini juga memberikan kinerja dan latensi yang konsisten untuk beban kerja hibrida. Diagram berikut memberikan salah satu contoh pendekatan lingkungan hibrida.



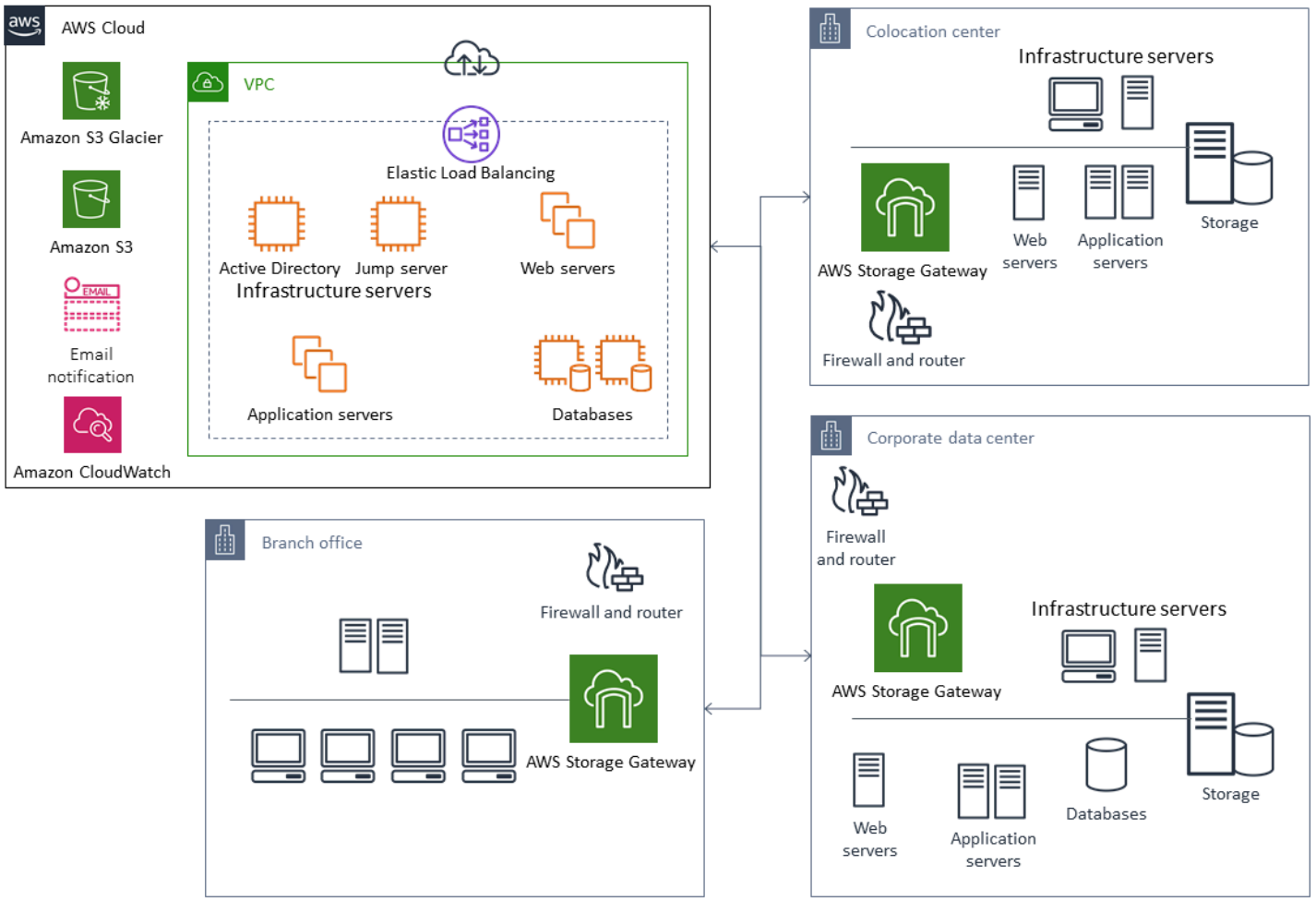
Solusi perlindungan data yang dirancang dengan baik biasanya menggunakan kombinasi opsi yang dijelaskan dalam solusi cloud-native dan lokal dalam panduan ini. Banyak ISV menyediakan solusi pencadangan dan pemulihan terdepan di pasar untuk infrastruktur lokal dan telah memperluas solusi mereka untuk mendukung pendekatan hybrid.

Memindahkan solusi manajemen cadangan terpusat ke cloud untuk ketersediaan yang lebih tinggi

Dengan menggunakan investasi solusi manajemen cadangan yang ada AWS, Anda dapat meningkatkan ketahanan dan arsitektur pendekatan Anda. Anda mungkin memiliki server cadangan utama dan satu atau beberapa server media atau penyimpanan yang terletak di lokasi di beberapa lokasi yang dekat dengan server dan layanan yang mereka lindungi. Dalam hal ini, pertimbangkan untuk memindahkan server cadangan utama ke instans EC2 untuk melindunginya dari bencana lokal dan untuk ketersediaan tinggi.

Untuk mengelola aliran data cadangan, Anda dapat membuat satu atau beberapa server media pada instans EC2 di Wilayah yang sama dengan server yang akan mereka lindungi. Server media di dekat instans EC2 menghemat uang Anda pada transfer internet. Saat Anda membuat cadangan ke Amazon S3, server media meningkatkan kinerja pencadangan dan pemulihan secara keseluruhan.

Anda juga dapat menggunakan Storage Gateway untuk menyediakan akses cloud terpusat ke data dari pusat data dan kantor yang tersebar secara geografis. Misalnya, gateway file memberi Anda akses latensi rendah sesuai permintaan ke data yang disimpan untuk alur kerja aplikasi yang dapat menjangkau dunia. AWS Anda dapat menggunakan fitur seperti penyegaran cache untuk menyegarkan data di lokasi yang didistribusikan secara geografis sehingga konten dapat dengan mudah dibagikan di seluruh kantor Anda.


AWS Cloud
Amazon S3 Glacier
Amazon S3
Email notification
Amazon CloudWatch
VPC
Elastic Load Balancing
Active Directory
Jump server
Web servers
Infrastructure servers
Application servers
Databases
Colocation center
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Storage
Firewall and router
Corporate data center
Firewall and router
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Databases
Storage
Branch office
Firewall and router
AWS Storage Gateway

Pemulihan bencana dengan AWS

Pendekatan pencadangan dan pemulihan serta layanan dan teknologi pendukung dapat digunakan untuk menerapkan solusi pemulihan bencana (DR) Anda. Banyak perusahaan menggunakan AWS Cloud untuk backup dan restore dan sebagai situs DR. AWS menyediakan sejumlah layanan dan fitur yang mendukung DR dan kelangsungan bisnis.

Topik

- DR di tempat ke AWS
- DR untuk beban kerja cloud-native

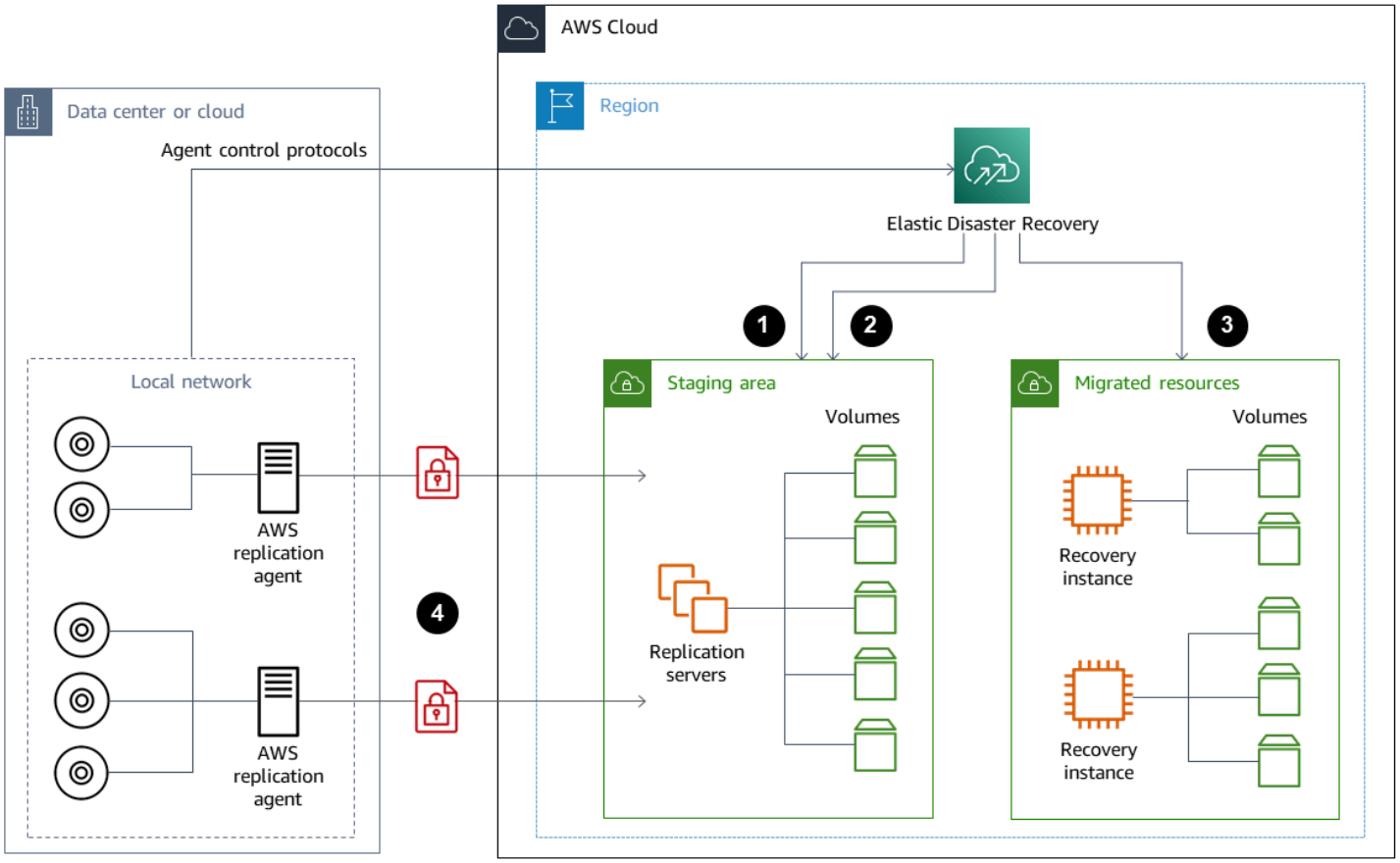
DR di tempat ke AWS

Menggunakan AWS lingkungan pemulihan bencana (DR) di luar lokasi untuk beban kerja lokal adalah skenario hibrida yang umum. Tentukan tujuan DR Anda, termasuk waktu pemulihan yang diperlukan dan tujuan titik pemulihan, sebelum memilih teknologi untuk digunakan. Untuk membantu definisi ini, Anda dapat menggunakan daftar periksa rencana DR.

Ada sejumlah opsi yang tersedia untuk membantu Anda mengatur dan menyediakan lingkungan DR dengan cepat AWS. Pastikan Anda memperhitungkan semua dependensi beban kerja Anda, dan uji rencana dan solusi DR Anda secara menyeluruh dan teratur untuk memverifikasi integritasnya.

AWS menyediakan AWS Elastic Disaster Recoveryuntuk membuat replika lengkap server lokal Anda, termasuk volume root dan sistem operasi, aktif. AWS Elastic Disaster Recovery terus mereplikasi alat berat Anda menjadi area pementasan berbiaya rendah di akun AWS target Anda dan lebih disukai. Wilayah AWS Replikasi tingkat blok adalah replika yang tepat dari penyimpanan server Anda termasuk sistem operasi, konfigurasi status sistem, database, aplikasi, dan file. Jika ada bencana, Anda dapat menginstruksikan Elastic Disaster Recovery untuk meluncurkan ribuan mesin Anda dengan cepat dalam kondisi yang disediakan sepenuhnya dalam beberapa menit.

Elastic Disaster Recovery menggunakan agen yang diinstal pada setiap server lokal Anda. Agen menyinkronkan status server lokal Anda dengan ekuivalen Amazon EC2 bertenaga rendah yang sedang berjalan. AWS Anda juga dapat mengotomatiskan proses failover dan failback DR Anda dengan Elastic Disaster Recovery. Mengotomatiskan proses failover dan failback Anda dapat membantu Anda mencapai tujuan waktu pemulihan (RTO) yang lebih rendah dan lebih konsisten.



1. Pelaporan status server replikasi
2. Sumber daya area pementasan secara otomatis dibuat dan dihentikan
3. Instans pemulihan diluncurkan dengan RTO menit dan RPO detik
4. Replikasi tingkat blok berkelanjutan (dikompresi dan dienkripsi)

Penting untuk menguji proses DR dan memverifikasi bahwa lingkungan pementasan langsung tidak menimbulkan konflik dengan lingkungan lokal. Misalnya, konfirmasikan bahwa lisensi yang sesuai tersedia dan berfungsi di lingkungan DR lokal, pementasan, dan yang dimulai. Juga konfirmasikan bahwa setiap proses tipe pekerja yang mungkin melakukan polling dan menarik pekerjaan dari database pusat dikonfigurasi dengan tepat untuk menghindari tumpang tindih atau konflik. Dalam proses DR Anda, sertakan langkah-langkah yang diperlukan yang harus dilakukan sebelum instance server pemulihan Anda online. Juga termasuk langkah-langkah untuk melakukan setelah instance server pemulihan online dan tersedia. Anda dapat menggunakan solusi seperti solusi Otomatisasi AWS Elastic Disaster Recovery Rencana atau pendekatan lain untuk membantu Anda mengotomatiskan rencana DR Anda.

Anda dapat menggunakan gateway volume Storage Gateway untuk menyediakan server lokal dengan volume berbasis Internet. Volume ini juga dapat dengan cepat disediakan untuk digunakan dengan Amazon EC2 menggunakan snapshot Amazon EBS. Secara khusus, gateway volume tersimpan menyediakan aplikasi lokal Anda dengan akses latensi rendah ke seluruh kumpulan datanya. Gerbang volume juga menyediakan cadangan berbasis snapshot tahan lama yang dapat dipulihkan untuk penggunaan di tempat atau untuk digunakan dengan Amazon EC2. Anda dapat menjadwalkan point-in-time snapshot berdasarkan tujuan titik pemulihan (RPO) untuk beban kerja Anda.

> **Important**
>
> Volume gateway volume dimaksudkan untuk digunakan sebagai volume data dan bukan sebagai volume boot.

Anda dapat menggunakan Amazon EC2 Amazon Machine Image (AMI) dengan konfigurasi yang cocok dengan server lokal dan menentukan volume data secara terpisah. Setelah Anda mengonfigurasi dan menguji AMI, berikan instans EC2 dari AMI beserta volume data berdasarkan snapshot gateway volume. Pendekatan ini mengharuskan Anda untuk menguji lingkungan Anda secara menyeluruh untuk memverifikasi bahwa instans EC2 Anda beroperasi dengan benar, terutama untuk beban kerja Windows.

DR untuk beban kerja cloud-native

Pertimbangkan bagaimana beban kerja cloud-native Anda selaras dengan tujuan DR Anda. AWS menyediakan beberapa Availability Zone di Wilayah di seluruh dunia. Banyak perusahaan yang menggunakan AWS Cloud menyelaraskan arsitektur beban kerja mereka dan tujuan DR untuk menahan hilangnya Availability Zone. Pilar Keandalan dalam Kerangka AWS Well-Architected mendukung praktik terbaik ini. Anda dapat merancang beban kerja Anda dan dependensi layanan dan aplikasinya untuk menggunakan beberapa Availability Zone. Anda kemudian dapat mengotomatiskan DR Anda dan mencapai tujuan DR Anda dengan intervensi minimal atau tanpa intervensi.

Namun, dalam praktiknya, Anda mungkin menemukan bahwa Anda tidak dapat membuat arsitektur yang berlebihan, aktif, dan otomatis untuk semua komponen Anda. Periksa setiap lapisan arsitektur Anda untuk menentukan proses DR yang diperlukan untuk mencapai tujuan Anda. Ini mungkin berbeda dari beban kerja ke beban kerja, dengan persyaratan arsitektur dan layanan yang berbeda.

Panduan ini mencakup pertimbangan dan opsi untuk Amazon EC2. Untuk AWS layanan lain, Anda dapat merujuk ke AWS dokumentasi untuk menentukan ketersediaan tinggi dan opsi DR.

DR untuk Amazon EC2 dalam satu Availability Zone

Cobalah untuk merancang beban kerja Anda untuk secara aktif mendukung dan melayani klien dari beberapa Availability Zone. Anda dapat menggunakan Amazon EC2 Auto Scaling dan Elastic Load Balancing untuk mencapai arsitektur server Multi-AZ untuk Amazon EC2 dan layanan lainnya.

Jika arsitektur Anda memiliki instans EC2 yang tidak dapat diseimbangkan beban dan hanya dapat menjalankan satu instance pada saat tertentu, Anda dapat menggunakan salah satu opsi berikut.

- Buat grup Auto Scaling yang memiliki ukuran minimum, maksimum, dan yang diinginkan sebesar 1 dan dikonfigurasi untuk beberapa Availability Zone. Buat AMI yang dapat digunakan untuk mengganti instance jika gagal. Pastikan Anda menentukan otomatisasi dan konfigurasi yang tepat sehingga instance yang baru disediakan dari AMI dapat dikonfigurasi secara otomatis dan menyediakan layanan. Buat penyeimbang beban yang menunjuk ke grup Auto Scaling dan dikonfigurasi untuk beberapa Availability Zone. Secara opsional, buat alias Amazon Route 53 yang mengarah ke titik akhir penyeimbang beban.
- Buat catatan Route 53 untuk instans aktif Anda dan minta klien Anda terhubung menggunakan catatan ini. Buat skrip yang membuat AMI baru dari instans aktif Anda dan gunakan AMI untuk menyediakan instans EC2 baru dalam status berhenti di Availability Zone terpisah. Konfigurasikan skrip untuk dijalankan secara berkala dan untuk menghentikan instance yang dihentikan sebelumnya. Jika ada kegagalan Availability Zone, mulai instance cadangan Anda di Availability Zone alternatif Anda. Kemudian perbarui catatan Route 53 untuk menunjuk ke instance baru ini.

Uji solusi Anda secara menyeluruh dengan mensimulasikan kegagalan yang dirancang untuk dilindungi oleh solusi. Pertimbangkan juga pembaruan yang dibutuhkan solusi DR Anda saat arsitektur beban kerja Anda berubah.

DR untuk Amazon EC2 dalam kegagalan regional

Pelanggan dengan persyaratan ketersediaan yang sangat tinggi (misalnya, aplikasi penting misi yang tidak dapat mentolerir waktu henti apa pun) dapat menggunakan AWS di beberapa Wilayah untuk memberikan ketahanan lebih lanjut terhadap masalah di tingkat Wilayah. Pelanggan harus mempertimbangkan dengan cermat kompleksitas, biaya, dan upaya yang diperlukan untuk menetapkan dan memelihara rencana DR Multi-wilayah terhadap manfaatnya. AWS menyediakan fitur yang mendukung arsitektur Multi-wilayah untuk ketersediaan global, failover, dan DR. Panduan

ini mencakup beberapa fitur yang tersedia yang khusus untuk pencadangan dan pemulihan untuk Amazon EC2.

AWS Snapshot AMI dan Amazon EBS adalah sumber daya regional yang dapat digunakan untuk menyediakan instans baru dalam satu Wilayah. Namun, Anda dapat menyalin snapshot dan AMI Anda ke Wilayah lain dan menggunakannya untuk menyediakan instance baru di Wilayah tersebut. Untuk mendukung rencana DR kegagalan regional, Anda dapat mengotomatiskan proses menyalin AMI dan snapshot ke Wilayah lain. AWS Backup dan Amazon Data Lifecycle Manager mendukung penyalinan lintas wilayah sebagai bagian dari konfigurasi cadangan Anda.

AWS Elastic Disaster Recoverydapat digunakan untuk mengotomatisasi dan terus mereplikasi server Amazon EC2 Anda di satu Wilayah ke Wilayah DR alternatif. Elastic Disaster Recovery dapat menyederhanakan pendekatan DR Multi-wilayah Anda dan membantu Anda menguji secara teratur paket Amazon EC2 DR Lintas wilayah Anda dengan menggunakan latihan. Elastic Disaster Recovery dapat membantu ketika pencadangan dan pemulihan tidak dapat memenuhi tujuan RTO dan RPO Anda. Elastic Disaster Recovery dapat membantu Anda menurunkan RTO ke menit dan RPO Anda ke kisaran sub-detik.

Solusi apa pun yang Anda gunakan, Anda harus menentukan proses penyediaan, failover, dan failback yang akan digunakan jika terjadi pemadaman. Anda dapat menggunakan Route 53 dengan pemeriksaan kesehatan dan failover Sistem Nama Domain untuk membantu mendukung solusi Anda.

Membersihkan backup

Untuk mengurangi biaya, bersihkan cadangan yang tidak lagi diperlukan untuk tujuan pemulihan atau retensi. Anda dapat menggunakanAWS Backupdan Amazon Data Lifecycle Manager untuk mengotomatiskan kebijakan penyimpanan Anda untuk sebagian cadangan Anda. Namun, bahkan dengan alat-alat ini di tempat, Anda masih memerlukan pendekatan pembersihan untuk backup yang diambil secara terpisah.

Strategi penandaan adalah prasyarat untuk strategi pembersihan. Gunakan penandaan untuk mengidentifikasi sumber daya yang harus dibersihkan, memberi tahu pemilik dengan tepat, dan mengotomatiskan proses pembersihan Anda. Cadangan yang dibuat olehAWSmemiliki tanggal pembuatan yang selaras dengannya, tetapi penandaan penting untuk mengkorelasikan cadangan dengan beban kerja, persyaratan retensi, dan identifikasi titik pemulihan.

Anda dapat menerapkan proses pembersihan untuk snapshot menggunakan otomatisasi. Misalnya, Anda dapat memindai akun Anda untuk snapshot dan menentukan apakah volume yang sesuai berada dalam keadaan terlampir atau status yang tersedia. Anda dapat memfilter hasil lebih lanjut pada ambang waktu yang Anda tentukan. Dengan menggunakan tag yang dilampirkan ke volume, Anda dapat secara otomatis mengirim email ke pemilik snapshot, dan memperingatkan mereka bahwa snapshot mereka telah dijadwalkan untuk dihapus. Remediasi otomatis ini dapat diimplementasikan dengan menggunakanAWS Configaturan, script menggunakanAWS CLI, atau fungsi Lambda menggunakanAWSSDK.

Systems Manager menyediakanAWS DeleteebsVolumeSnapshotsdanAWS-DeleteSnapshotdokumen untuk membantu Anda memulai dan mengotomatiskan pembersihan snapshot Amazon EBS. Anda juga dapat menggunakanAWS CLIdanAWSSDK untuk mengotomatiskan pembersihan lainnyaAWSsumber daya seperti snapshot Amazon RDS.

FAQ cadangan dan pemulihan

Jadwal cadangan apa yang harus saya pilih?

Tentukan frekuensi jadwal cadangan yang sejalan dengan tujuan titik pemulihan (RPO) Anda. Tentukan waktu cadangan saat beban kerja Anda berada di bawah jumlah beban paling sedikit dan kapan dampak pengguna dapat dikurangi. Buat sebuahpoint-in-timesnapshot setiap kali Anda akan membuat perubahan signifikan pada beban kerja Anda.

Apakah saya perlu membuat cadangan di akun pengembangan saya?

Uji potensi melanggar perubahan di akun pengembangan untuk beban kerja Anda dan buat cadangan sebelum melakukan perubahan yang melanggar. Anda mungkin memiliki lebih banyakpoint-in-timebackup recovery (PITR) di akun pengembangan dan non-produksi Anda dari aktivitas pengembangan dan pengujian.

Dapatkah saya meningkatkan aplikasi dan terus menggunakan volume EBS saat snapshot dibuat tanpa dampak apa pun?

Snapshot terjadi secara asinkron;point-in-timesnapshot dibuat segera, tetapi status snapshot tertunda sampai semua blok yang dimodifikasi telah ditransfer ke Amazon S3. Untuk snapshot awal yang besar atau snapshot berikutnya di mana banyak blok telah berubah, transfer dapat memakan waktu beberapa jam. Saat mentransfer, snapshot yang sedang berlangsung tidak terpengaruh oleh pembacaan dan penulisan yang sedang berlangsung ke volume. Untuk informasi lebih lanjut, lihat dokumentasi AWS.

Langkah selanjutnya

Mulailah dengan mengevaluasi, menerapkan, dan menguji pendekatan pencadangan dan pemulihan Anda di lingkungan non-produksi. Penting untuk menguji proses pemulihan Anda secara menyeluruh dan memvalidasi bahwa beban kerja Anda yang dipulihkan beroperasi seperti yang diharapkan.

Uji proses pemulihan untuk satu komponen dalam arsitektur Anda selain semua komponen dalam arsitektur Anda. Validasi waktu pemulihan untuk masing-masing. Juga memvalidasi dampak proses pencadangan dan pemulihan Anda pada dependensi hulu dan hilir. Konfirmasikan dampak pemadaman layanan apa pun pada dependensi hulu Anda dan konfirmasikan dampak hilir pada cadangan Anda.

Sumber daya tambahan

Sumber daya AWS

- AWS Bimbingan Preskriptif
- Dokumentasi AWS
- Referensi umum AWS
- Glosarium AWS

Layanan AWS

- AWS Backup
- Amazon CloudWatch
- CloudWatch Acara Amazon
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- IAM
- Amazon RDS
- Amazon S3
- Storage Gateway
- AWS Systems Manager

Sumber daya lainnya

- Backup dan Recovery dengan AWS Backup (solusi)
- Pemulihan Bencana Beban Kerja di AWS: Pemulihan di Cloud (whitepaper)
- Seri Pemulihan Bencana (posting blog AWS Architecture)
- Daftar Periksa Rencana DR
- Pendekatan Backup dan Recovery Using AWS (technical paper — diarsipkan)
- Memulai dengan AWS Backup

- AWS Marketplace — Backup dan Restore

Riwayat dokumen

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
Informasi yang diperbarui	Panduan yang diperbarui di bagian Amazon S3.	Juni 28, 2024
Informasi yang diperbarui	Informasi yang diperbarui di AWS bagian DR to lokal.	13 April 2023
Ditambahkan bagian	Menambahkan panduan dan langkah-langkah untuk membuat atau memulihkan instance dari snapshot.	7 Maret 2023
Menambahkan informasi tentang Elastic Disaster Recovery dan menambahkan klarifikasi	Dalam pemulihan Bencana dengan AWS dan Memilih AWS layanan untuk bagian perlindungan data, menambahkan informasi tentang AWS Elastic Disaster Recovery. Di pencadangan dan pemulihan Amazon EC2 dengan snapshot dan AMI, Mempersiapkan volume EBS sebelum membuat snapshot atau AMI, dan Memulihkan dari snapshot Amazon EBS atau bagian AMI, menambahkan klarifikasi. Ditambahkan ke FAQ Backup dan pemulihan.	19 Januari 2023
Menambahkan link	Menambahkan tautan ke dokumentasi Amazon Data	31 Oktober 2022

	Lifecycle Manager di bagian Amazon Data Lifecycle Manager.	
Informasi yang diperbarui	Memperbarui informasi tentang memulihkan volume.	30 Agustus 2022
Informasi yang diperbarui dan menambahkan bagian baru	Di bagian Memilih AWS layanan untuk perlindungan data, menambahkan layanan. Menambahkan bagian Backup dan recovery menggunakan AWS Backup. Di bagian Backup dan recovery menggunakan Amazon S3 dan Amazon S3 Glacier, menambahkan informasi tentang kelas penyimpanan Amazon S3 Glacier baru. Di bagian Backup dan recovery untuk Amazon EC2 dengan volume EBS, tambahkan tautan ke dokumentasi dan informasi tambahan. Di bagian Backup dan pemulihan AWS layanan cloud-native, tambahkan rekomendasi untuk digunakan . AWS Backup Di bagian Sumber daya tambahan, tambahkan sumber daya.	28 Januari 2022

Informasi yang diperbarui	Menambahkan informasi tentang pengaturan kelas penyimpanan ke bagian S3 Glacier Flexible Retrieval . Menambahkan informasi tentang mengambil snapshot ke cadangan dan pemulihan Amazon EC2 dengan snapshot dan bagian AMI.	9 September 2021
Informasi yang diperbarui	Di AWS Backupbagian tersebut, menambahkan informasi tentang AWS layanan yang AWS Backup mendukung.	1 Juni 2021
Publikasi awal	—	29 Juli 2020

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: Migrasikan 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 instans 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 menyebabkan kerugian bagi 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

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.

Cloud Center of Excellence (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 CCoE 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 CCoE, 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. AWS CodeCommit 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 penyimpanan atau kelas 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, AWS Panorama menawarkan perangkat yang menambahkan CV ke jaringan kamera lokal, dan Amazon SageMaker menyediakan algoritme 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 Wilayah, 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 umumnya digambarkan sebagai pipa. CI/CD dapat 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 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 yang ada. 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 database.

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.

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.

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.

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.

G

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.

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 (OU). 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.

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 VPC masuk, keluar, dan inspeksi 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 selengkapnya, 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 VPC (dalam hal yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi 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 selengkapnya, 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.

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.

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 melalui API yang terdefinisi dengan baik 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 API ringan. 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 terbaik dan pelajaran yang dipetik 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 AWS dengan Layanan Migrasi 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 Mengurai 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 VPC masuk, keluar, dan inspeksi 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 kebijakanberbasis sumber daya), atau menentukan izin maksimum untuk semua akun dalam organisasi di (lihat kebijakan kontrol layanan). AWS Organizations

persistensi 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 pengoptimalan 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 oleh Desain

Pendekatan dalam rekayasa sistem yang memperhitungkan privasi di seluruh proses rekayasa.

zona host pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau beberapa VPC. 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.

pseudonimisasi

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

terbitkan/berlangganan (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).

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 hilangnya 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 prinsip 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). Jenis 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.

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.

PENIPUAN

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.

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 Amazon EC2, 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 SCP menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCP sebagai 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.

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 VPC dan jaringan lokal Anda. 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 VPC yang memungkinkan Anda 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 terkini 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 Kerangka Kualifikasi Beban Kerja AWS.

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.

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.