AWS Whitepaper

AWSBatas Isolasi Kesalahan

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

AWSBatas Isolasi Kesalahan: AWS Whitepaper

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan kekayaan masing-masing pemiliknya, yang mungkin atau mungkin tidak berafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Abstrak dan Pendahuluan ... 1
Abstrak ... 1
Apakah Anda Well-Architected? ... 1
Pengantar ... 1
AWSInfrastruktur ... 3
Zona Ketersediaan ... 3
Wilayah ... 4
AWSLocal Zones ... 5
AWS Outposts ... 5
Poin kehadiran ... 6
Partisi ... 7
Kontrol pesawat dan pesawat data ... 7
Stabilitas statis ... 8
Ringkasan ... 9
AWS jenis layanan ... 10
Layanan Zonal ... 10
Layanan regional ... 13
Layanan global ... 14
Layanan global yang unik berdasarkan partisi ... 15
Layanan global di jaringan edge ... 16
Operasi Wilayah Tunggal Global ... 17
Layanan yang menggunakan endpoint global default ... 21
Ringkasan layanan global ... 23
Kesimpulan ... 27
Lampiran A - Panduan layanan partisi ... 28
AWSIAM ... 28
AWS Organizations ... 28
AWSManajemen Akun ... 29
Pengendali Pemulihan Aplikasi Route 53 ... 30
AWSNetwork Manager ... 30
Rute 53 DNS Pribadi ... 31
Lampiran B - Panduan layanan global jaringan Edge ... 32
Route 53 ... 32
Amazon CloudFront ... 33

Certificate Manager Amazon 33
AWSFirewall Aplikasi Web (WAF) dan WAF Classic 33
AWSAkselerator Global Accelerator 34
Amazon Shield Advanced 34
Lampiran C - Layanan Single-Region 35
Kontributor 36
Revisi dokumen 37
Glosarium AWS 38
Pemberitahuan 39
..... xl

Batas Isolasi Kesalahan AWS

Tanggal penerbitan: 16 November 2022 () Revisi dokumen

Abstrak

Amazon Web Services (AWS) menyediakan batasan isolasi yang berbeda, seperti Availability Zones (AZ), Wilayah, bidang kontrol, dan bidang data. paper ini menjelaskan bagaimana AWS menggunakan batas-batas ini untuk menciptakan layanan zonal, Regional, dan global. Ini juga mencakup panduan preskriptif tentang cara mempertimbangkan dependensi pada layanan yang berbeda ini dan cara meningkatkan ketahanan beban kerja yang Anda bangun menggunakannya.

Apakah Anda Well-Architected?

Kerangka Kerja AWS Well-Architected membantu Anda memahami pro dan kontra dari keputusan yang Anda buat saat membangun sistem di cloud. Enam pilar Kerangka ini memungkinkan Anda mempelajari praktik terbaik arsitektur untuk merancang dan mengoperasikan sistem yang andal, aman, efisien, hemat biaya, dan berkelanjutan. Dengan menggunakan AWS Well-Architected Tool, tersedia tanpa biaya di Konsol Manajemen AWS, Anda dapat meninjau beban kerja Anda terhadap praktik terbaik ini dengan menjawab serangkaian pertanyaan untuk setiap pilar.

Untuk panduan ahli dan praktik terbaik lainnya untuk arsitektur cloud Anda—referensi penerapan arsitektur, diagram, dan whitepaper—lihat Architecture Center. AWS

Pengantar

AWSmengoperasikan infrastruktur global untuk menyediakan layanan cloud yang membantu pelanggan menerapkan beban kerja dengan cara yang fleksibel, aman, dapat diskalakan, dan sangat tersedia. AWSInfrastruktur menggunakan beberapa konstruksi isolasi kesalahan untuk membantu pelanggan mencapai tujuan ketahanan mereka. Batas isolasi kesalahan ini memungkinkan pelanggan merancang beban kerja mereka untuk memanfaatkan ruang lingkup penahanan dampak yang dapat diprediksi yang mereka berikan. Penting juga untuk memahami bagaimana AWS layanan dirancang menggunakan batas-batas ini sehingga Anda dapat membuat pilihan yang disengaja tentang dependensi yang Anda pilih untuk beban kerja Anda.

paper ini pertama-tama akan merangkum infrastruktur AWS global dan batasan isolasi kesalahan yang diberikannya, serta beberapa pola yang digunakan untuk merancang layanan kami. Dengan

menggunakan dasar pemahaman ini, paper selanjutnya akan menguraikan cakupan AWS layanan yang berbeda: zonal, Regional, dan global. Ini juga akan menyajikan praktik terbaik untuk membangun arsitektur yang menggunakan batas isolasi ini dan cakupan layanan yang berbeda untuk meningkatkan ketahanan beban kerja yang Anda jalankan. AWS Secara khusus, ini memberikan panduan preskriptif tentang bagaimana mengambil dependensi pada layanan global sambil meminimalkan titik kegagalan tunggal. Ini akan membantu Anda membuat pilihan informasi tentang AWS dependensi Anda dan bagaimana Anda merancang beban kerja Anda untuk ketersediaan tinggi (HA) dan pemulihan bencana (DR).

AWSInfrastruktur

Bagian ini menyajikan ringkasan infrastruktur AWS global dan batas-batas isolasi kesalahan yang disediakannya. Selain itu, bagian ini akan memberikan gambaran umum tentang konsep pesawat kontrol dan bidang data, yang merupakan perbedaan penting dalam cara AWS mendesain layanannya. Informasi ini memberikan dasar untuk memahami bagaimana batas isolasi kesalahan dan bidang kontrol layanan dan bidang data berlaku untuk jenis AWS layanan yang kita bahas di bagian selanjutnya.

Topik

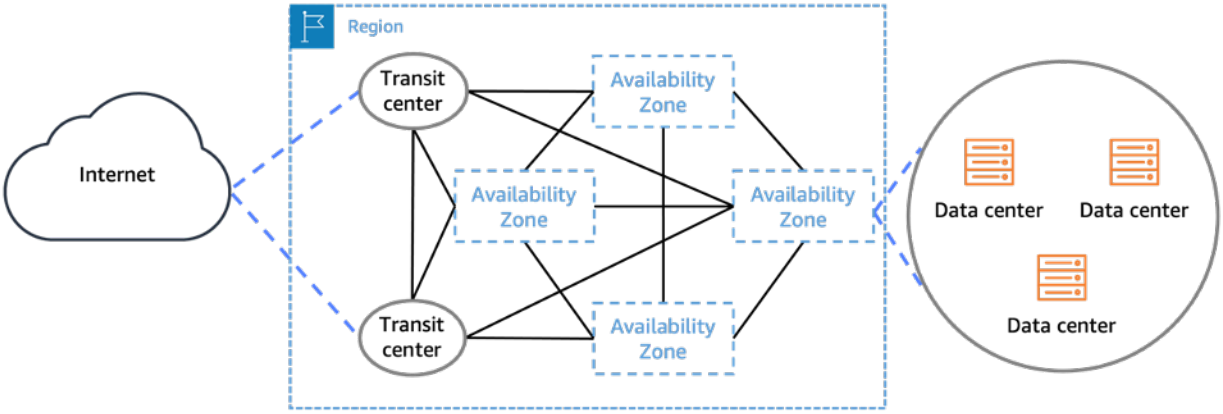
- Zona Ketersediaan
- Wilayah
- AWSLocal Zones
- AWS Outposts
- Poin kehadiran
- Partisi
- Kontrol pesawat dan pesawat data
- Stabilitas statis
- Ringkasan

Zona Ketersediaan

AWSmengoperasikan lebih dari 100 Availability Zone di beberapa Wilayah di seluruh dunia (angka saat ini dapat ditemukan di sini: Infrastruktur AWS Global). Availability Zone adalah satu atau lebih pusat data diskrit dengan infrastruktur daya, jaringan, dan konektivitas independen dan redundan dalam suatu sistem. Wilayah AWS Availability Zone di suatu Wilayah sangat jauh satu sama lain, hingga 60 mil (~100 km) untuk mencegah kegagalan yang berkorelasi, tetapi cukup dekat untuk menggunakan replikasi sinkron dengan latensi milidetik satu digit. Mereka dirancang untuk tidak secara bersamaan terkena dampak skenario nasib bersama seperti listrik utilitas, gangguan air, isolasi serat, gempa bumi, kebakaran, tornado, atau banjir. Titik kegagalan umum, seperti generator dan peralatan pendingin, tidak dibagi di seluruh Availability Zone dan dirancang untuk dipasok oleh gardu listrik independen. Saat AWS menerapkan pembaruan ke layanannya, penerapan ke Availability Zone di Wilayah yang sama dipisahkan tepat waktu untuk mencegah kegagalan yang berkorelasi.

Semua Availability Zone di suatu Wilayah saling berhubungan dengan jaringan bandwidth tinggi, latensi rendah, melalui serat metro khusus yang sepenuhnya redundan. Setiap Availability Zone di suatu Wilayah terhubung ke internet melalui dua pusat transit di mana AWS rekan-rekan dengan beberapa penyedia internet tingkat-1 (untuk informasi lebih lanjut, lihat Ikhtisar Amazon Web Services).

Fitur-fitur ini memberikan isolasi yang kuat dari Availability Zone satu sama lain, yang kami sebut sebagai Availability Zone Independence (AZI). Konstruksi logis Availability Zones dan konektivitasnya ke internet digambarkan pada gambar berikut.



Availability Zones terdiri dari satu atau lebih pusat data fisik yang terhubung secara berlebihan satu sama lain dan internet

Wilayah

Masing-masing Wilayah AWS terdiri dari beberapa Availability Zone yang independen dan terpisah secara fisik dalam suatu wilayah geografis. Semua Wilayah saat ini memiliki tiga atau lebih Availability Zone. Daerah itu sendiri terisolasi dan independen dari Wilayah lain dengan beberapa pengecualian yang dicatat kemudian dalam dokumen ini (lihat operasi Wilayah Tunggal Global). Pemisahan antar Wilayah ini membatasi kegagalan layanan, ketika terjadi, ke satu Wilayah. Operasi normal Wilayah Lain tidak terpengaruh dalam kasus ini. Selain itu, sumber daya dan data yang Anda buat di satu Wilayah tidak ada di Wilayah lain kecuali Anda secara eksplisit menggunakan fitur replikasi atau salin yang ditawarkan oleh AWS layanan atau mereplikasi sumber daya sendiri.

Wilayah AWS saat ini dan yang direncanakan per Desember 2022

AWSLocal Zones

AWSLocal Zones adalah jenis penyebaran infrastruktur yang menempatkan komputasi, penyimpanan, database, dan AWSlayanan pilihan lainnya dekat dengan populasi besar dan pusat industri. Anda dapat menggunakan AWS layanan, seperti layanan komputasi dan penyimpanan, di Zona Lokal untuk menjalankan aplikasi latensi rendah di edge atau menyederhanakan migrasi cloud hybrid. Local Zones memiliki masuknya internet lokal dan keluar untuk mengurangi latensi, tetapi juga terhubung ke Wilayah induknya melalui jaringan pribadi Amazon yang redundan dan bandwidth tinggi, memberikan aplikasi yang berjalan di Local Zones AWS akses cepat, aman, dan mulus ke berbagai layanan.

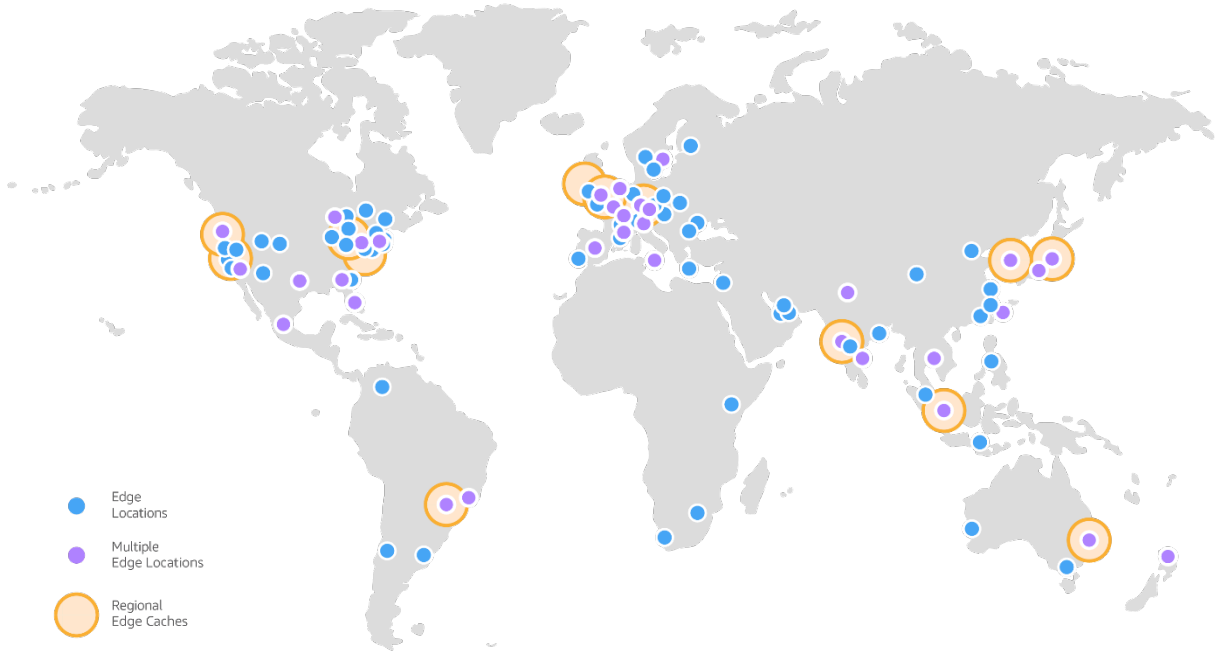
AWS Outposts

AWS Outpostsadalah rangkaian solusi terkelola penuh yang memberikan AWS infrastruktur dan layanan ke hampir semua lokasi lokal atau tepi untuk pengalaman hybrid yang benar-benar konsisten. Solusi Outposts memungkinkan Anda memperluas dan menjalankan AWS layanan asli lokal, dan tersedia dalam berbagai faktor bentuk, dari server Outposts 1U dan 2U hingga rak Outposts 42U, dan beberapa penerapan rak.

DenganAWS Outposts, Anda dapat menjalankan AWSlayanan tertentu secara lokal dan terhubung ke berbagai layanan yang tersedia di indukWilayah AWS. AWS Outpostsadalah rak komputasi dan penyimpanan yang dikelola sepenuhnya dan dapat dikonfigurasi yang dibangun dengan perangkat keras AWS yang dirancang yang memungkinkan pelanggan menjalankan komputasi dan penyimpanan di tempat, sambil terhubung dengan mulus ke beragam layanan AWS di cloud.

Poin kehadiran

Selain Availability Zones Wilayah AWS dan Availability Zones, AWS juga mengoperasikan jaringan point of presence (PoP) yang didistribusikan secara global. PoPs Host Amazon ini CloudFront, jaringan pengiriman konten (CDN); Amazon Route 53, layanan resolusi Sistem Nama Domain publik (DNS); dan AWS Global Accelerator (AGA), layanan pengoptimalan jaringan tepi. Jaringan edge global saat ini terdiri dari lebih dari 410 PoPs, termasuk lebih dari 400 Lokasi Edge, dan 13 cache tingkat menengah regional di lebih dari 90 kota di 48 negara (status saat ini dapat ditemukan di sini: Fitur CloudFront Utama Amazon).



Jaringan tepi CloudFront global Amazon

Setiap PoP diisolasi dari yang lain, yang berarti kegagalan yang mempengaruhi satu PoP atau wilayah metropolitan tidak berdampak pada jaringan global lainnya. AWSJaringan rekan-rekan dengan ribuan operator telekomunikasi Tier 1/2/3 secara global, terhubung dengan baik dengan semua jaringan akses utama untuk kinerja optimal, dan memiliki ratusan terabit kapasitas yang

digunakan. Lokasi tepi terhubung ke Wilayah AWS melalui tulang punggung AWS jaringan, serat paralel 100GbE yang sepenuhnya berlebihan yang mengelilingi dunia dan terhubung dengan puluhan ribu jaringan untuk pengambilan asal yang lebih baik dan akselerasi konten dinamis.

Partisi

AWSmengelompokkan Wilayah menjadi partisi. Setiap Wilayah berada dalam satu partisi, dan setiap partisi memiliki satu atau lebih Wilayah. Partisi memiliki instance independen AWS Identity and Access Management (IAM) dan memberikan batas keras antara Wilayah di partisi yang berbeda. AWSDaerah komersial berada di `aws` partisi, Wilayah di China berada di `aws-cn` partisi, dan AWS GovCloud Wilayah berada di `aws-us-gov` partisi. Beberapa AWS layanan dirancang untuk menyediakan fungsionalitas Lintas wilayah, seperti Amazon S3 Cross-Region Replication atau AWSTransit Gateway Inter-Region peering. Jenis kemampuan ini hanya didukung antara Wilayah di partisi yang sama. Anda tidak dapat menggunakan kredensil IAM dari satu partisi untuk berinteraksi dengan sumber daya di partisi yang berbeda.

Kontrol pesawat dan pesawat data

AWSmemisahkan sebagian besar layanan ke dalam konsep bidang kontrol dan bidang data. Istilah-istilah ini berasal dari dunia jaringan, khususnya router. Bidang data router, yang merupakan fungsi utamanya, memindahkan paket berdasarkan aturan. Tetapi kebijakan perutean harus dibuat dan didistribusikan dari suatu tempat, dan di situlah bidang kontrol masuk.

Bidang kontrol menyediakan API administratif yang digunakan untuk membuat, membaca/mendeskripsikan, memperbarui, menghapus, dan mencantumkan sumber daya (CRUDL). Misalnya, berikut ini adalah semua tindakan bidang kontrol: meluncurkan instans Amazon Elastic Compute Cloud (Amazon EC2) baru, membuat bucket Amazon Simple Storage Service (Amazon S3), dan menjelaskan antrean Amazon Simple Queue Service (Amazon SQS). Saat Anda meluncurkan instans EC2, bidang kontrol harus melakukan beberapa tugas seperti menemukan host fisik dengan kapasitas, mengalokasikan antarmuka jaringan, menyiapkan volume Amazon Elastic Block Store (Amazon EBS), menghasilkan kredensil IAM, menambahkan aturan Grup Keamanan, dan banyak lagi. Bidang kontrol cenderung menjadi sistem orkestrasi dan agregasi yang rumit.

Bidang data adalah apa yang menyediakan fungsi utama layanan. Misalnya, berikut ini adalah semua bagian dari bidang data untuk setiap layanan yang terlibat: instans EC2 yang sedang berjalan itu sendiri, membaca dan menulis ke volume EBS, mendapatkan dan meletakkan objek dalam bucket S3, dan Route 53 menjawab kueri DNS dan melakukan pemeriksaan kesehatan.

Bidang data sengaja tidak terlalu rumit, dengan bagian yang bergerak lebih sedikit dibandingkan dengan bidang kontrol, yang biasanya menerapkan sistem alur kerja, logika bisnis, dan basis data yang kompleks. Hal ini membuat peristiwa kegagalan secara statistik lebih kecil kemungkinannya terjadi di bidang data versus bidang kontrol. Sementara data dan bidang kontrol berkontribusi pada keseluruhan operasi dan keberhasilan layanan, AWS menganggapnya sebagai komponen yang berbeda. Pemisahan ini memiliki manfaat kinerja dan ketersediaan.

Stabilitas statis

Salah satu karakteristik ketahanan AWS layanan yang paling penting adalah apa yang AWS disebut stabilitas statis. Apa arti istilah ini adalah bahwa sistem beroperasi dalam keadaan statis dan terus beroperasi seperti biasa tanpa perlu membuat perubahan selama kegagalan atau tidak tersedianya dependensi. Salah satu cara kami melakukan ini adalah dengan mencegah dependensi melingkar dalam layanan kami yang dapat menghentikan salah satu layanan tersebut agar tidak berhasil pulih. Cara lain kami melakukan ini adalah dengan mempertahankan status yang ada. Kami mempertimbangkan fakta bahwa pesawat kontrol secara statistik lebih mungkin gagal daripada pesawat data. Meskipun bidang data biasanya tergantung pada data yang datang dari bidang kontrol, pesawat data mempertahankan keadaan yang ada dan terus bekerja bahkan dalam menghadapi gangguan bidang kontrol. Akses pesawat data ke sumber daya, setelah disediakan, tidak memiliki ketergantungan pada bidang kontrol, dan oleh karena itu tidak terpengaruh oleh gangguan bidang kontrol apa pun. Dengan kata lain, bahkan jika kemampuan untuk membuat, memodifikasi, atau menghapus sumber daya terganggu, sumber daya yang ada tetap tersedia. Hal ini membuat pesawat AWS data stabil secara statis terhadap gangguan pada bidang kontrol. Anda dapat menerapkan pola yang berbeda agar stabil secara statis terhadap berbagai jenis kegagalan ketergantungan.

Contoh stabilitas statis dapat ditemukan di Amazon EC2. Setelah instans EC2 diluncurkan, itu sama tersedia seperti server fisik di pusat data. Itu tidak bergantung pada API bidang kontrol apa pun untuk tetap berjalan, atau untuk mulai berjalan lagi setelah reboot. Properti yang sama berlaku untuk AWS sumber daya lain seperti VPC, bucket dan objek Amazon S3, dan volume Amazon EBS.

Stabilitas statis adalah konsep yang tertanam dalam bagaimana AWS mendesain layanannya, tetapi juga merupakan pola yang dapat digunakan oleh pelanggan. Faktanya, sebagian besar panduan praktik terbaik untuk menggunakan berbagai jenis AWS layanan dengan cara yang tangguh adalah menerapkan stabilitas statis untuk lingkungan produksi. Mekanisme pemulihan dan mitigasi yang paling andal adalah mekanisme yang membutuhkan perubahan paling sedikit untuk mencapai pemulihan. Alih-alih mengandalkan bidang kontrol EC2 untuk meluncurkan instans EC2 baru untuk pulih dari Availability Zone yang gagal, memiliki kapasitas ekstra yang telah disediakan sebelumnya

membantu mencapai stabilitas statis. Dengan demikian, menghilangkan dependensi pada bidang kontrol (API yang menerapkan perubahan pada sumber daya) di jalur pemulihan Anda membantu menghasilkan beban kerja yang lebih tangguh. Untuk detail selengkapnya tentang stabilitas statis, bidang kontrol, dan bidang data, lihat artikel Perpustakaan Pembangun Amazon Stabilitas statis menggunakan Availability Zones.

Ringkasan

AWSmenggunakan wadah kesalahan yang berbeda dalam infrastruktur kami untuk membuat isolasi kesalahan. Kontainer kesalahan infrastruktur inti adalah partisi, Wilayah, Zona Ketersediaan, bidang kontrol, dan bidang data. Selanjutnya, kita akan memeriksa berbagai jenis AWS layanan, bagaimana wadah kesalahan ini digunakan dalam desainnya, dan bagaimana Anda harus merancang beban kerja dengan mereka agar tangguh.

AWS jenis layanan

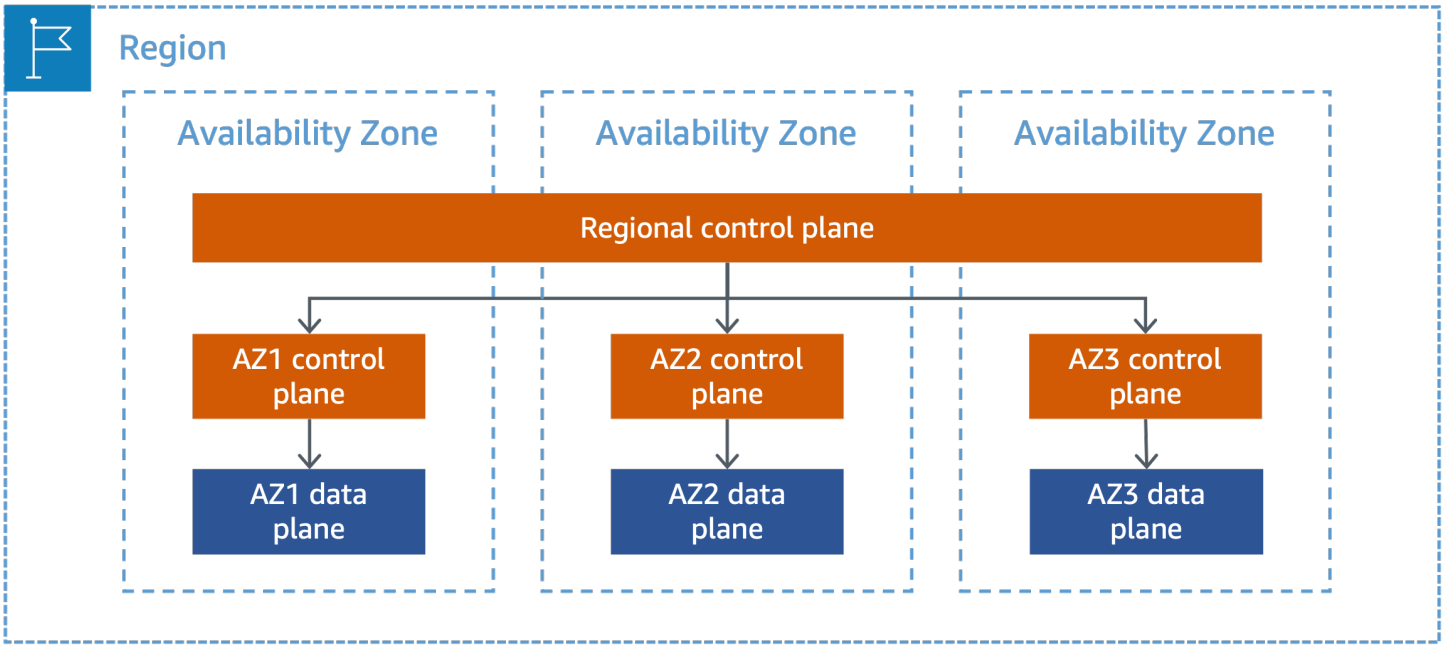
AWS mengoperasikan tiga kategori layanan yang berbeda berdasarkan batas isolasi kesalahan mereka: zona, Regional, dan global. Bagian ini akan menjelaskan secara lebih rinci bagaimana berbagai jenis layanan ini telah dirancang sehingga Anda dapat menentukan bagaimana kegagalan dalam layanan dari jenis layanan tertentu akan berdampak pada AWS beban kerja Anda berjalan. Ini juga memberikan panduan tingkat tinggi tentang cara merancang beban kerja Anda untuk menggunakan layanan ini dengan cara yang tangguh. Untuk layanan global, dokumen ini juga memberikan panduan preskriptif Lampiran A - Panduan layanan partisi dan Lampiran B - Panduan layanan global jaringan Edge yang dapat membantu Anda mencegah dampak pada beban kerja Anda dari gangguan bidang kontrol dalam AWS layanan, membantu Anda mengambil ketergantungan dengan aman pada layanan global sambil meminimalkan pengenalan satu titik kegagalan.

Topik

- Layanan Zonal
- Layanan regional
- Layanan global

Layanan Zonal

Availability Zone Independence (AZI) memungkinkan AWS untuk menawarkan layanan zona, seperti Amazon EC2 dan AmazonEBS. Layanan zonal adalah layanan yang menyediakan kemampuan untuk menentukan Availability Zone mana sumber daya digunakan. Layanan ini beroperasi secara independen di setiap Availability Zone dalam suatu Wilayah, dan yang lebih penting, gagal secara independen di setiap Availability Zone juga. Ini berarti bahwa komponen layanan dalam satu Availability Zone tidak mengambil dependensi pada komponen di Availability Zone lainnya. Kita dapat melakukan ini karena layanan zonal memiliki bidang data zona. Dalam beberapa kasus, seperti denganEC2, layanan ini juga mencakup bidang kontrol zona untuk operasi yang disejajarkan secara zonal, seperti meluncurkan instance. EC2 Untuk layanan tersebut, AWS juga menyediakan endpoint pesawat kontrol regional untuk memudahkan berinteraksi dengan layanan. Bidang kontrol regional juga menyediakan fungsionalitas cakupan regional serta berfungsi sebagai lapisan agregasi dan perutean di atas bidang kontrol zona. Ini ditunjukkan pada gambar berikut.



Layanan zona dengan bidang kontrol dan bidang data yang terisolasi secara zona

Availability Zones memberi pelanggan kemampuan untuk mengoperasikan beban kerja produksi yang lebih tersedia, toleran terhadap kesalahan, dan skalabel daripada yang mungkin dilakukan dari satu pusat data. Ketika beban kerja menggunakan beberapa Availability Zone, pelanggan akan lebih terisolasi dan terlindungi dari masalah yang berdampak pada infrastruktur fisik Availability Zone tunggal. Ini membantu pelanggan untuk membangun layanan yang berlebihan di seluruh Availability Zone dan, jika dirancang dengan benar, tetap beroperasi meskipun satu Availability Zone mengalami kegagalan. Pelanggan dapat memanfaatkan AZI untuk menciptakan beban kerja yang sangat tersedia dan tangguh. Menerapkan AZI dalam arsitektur Anda membantu Anda memulihkan dengan cepat dari kegagalan Availability Zone yang terisolasi karena sumber daya Anda dalam satu Availability Zone meminimalkan atau menghilangkan interaksi dengan sumber daya di Availability Zone lainnya. Ini membantu menghapus dependensi lintas Availability Zone yang menyederhanakan evakuasi Availability Zone. Lihat Pola Ketahanan Multi-AZ Tingkat Lanjut untuk detail selengkapnya tentang pembuatan mekanisme evakuasi Availability Zone. Selain itu, Anda dapat memanfaatkan Availability Zone lebih lanjut dengan mengikuti beberapa praktik terbaik yang sama yang AWS digunakan untuk layanannya sendiri, seperti hanya menerapkan perubahan ke Availability Zone tunggal pada satu waktu atau menghapus Availability Zone dari layanan jika perubahan di Availability Zone berjalan buruk.

Stabilitas statis juga merupakan konsep penting untuk arsitektur Multi-Availability Zone. Salah satu mode kegagalan yang harus Anda rencanakan dengan arsitektur Multi-Availability Zone adalah hilangnya Availability Zone, yang dapat mengakibatkan hilangnya kapasitas Availability Zone. Jika

Anda belum menyediakan kapasitas yang cukup untuk menangani hilangnya Availability Zone, ini dapat mengakibatkan kapasitas Anda yang tersisa kewalahan oleh beban saat ini. Selain itu, Anda harus bergantung pada bidang kontrol layanan zona yang Anda gunakan untuk mengganti kapasitas yang hilang, yang bisa kurang dapat diandalkan daripada desain yang stabil secara statis. Dalam hal ini, pra-penyediaan kapasitas ekstra yang cukup dapat membantu Anda stabil secara statis terhadap hilangnya domain kesalahan, seperti Availability Zone, dengan dapat melanjutkan operasi normal tanpa perlu perubahan dinamis.

Anda dapat memilih untuk menggunakan grup EC2 instans penskalaan otomatis yang diterapkan di beberapa Availability Zone untuk menskalakan masuk dan keluar secara dinamis, berdasarkan kebutuhan beban kerja Anda. Penskalaan otomatis berfungsi dengan baik untuk perubahan bertahap dalam penggunaan yang terjadi selama beberapa menit hingga puluhan menit. Namun, meluncurkan EC2 instance baru membutuhkan waktu, terutama jika instance Anda memerlukan bootstrap (seperti menginstal agen, binari aplikasi, atau file konfigurasi). Selama waktu ini, kapasitas Anda yang tersisa bisa kewalahan oleh beban saat ini. Selain itu, menerapkan instance baru melalui penskalaan otomatis bergantung pada bidang kontrol. EC2 Ini menyajikan trade-off: Agar stabil secara statis terhadap hilangnya satu Availability Zone, Anda perlu menyediakan EC2 instance yang cukup di Availability Zone lainnya untuk menangani beban yang telah digeser dari Availability Zone yang terganggu, alih-alih mengandalkan penskalaan otomatis untuk menyediakan instance baru. Namun, kapasitas ekstra pra-penyediaan dapat menimbulkan biaya tambahan.

Misalnya, selama operasi normal, anggap beban kerja Anda memerlukan enam instance untuk melayani lalu lintas pelanggan di tiga Availability Zone. Agar stabil secara statis terhadap satu kegagalan Availability Zone, Anda akan menerapkan tiga instance di setiap Availability Zone, dengan total sembilan. Jika satu instance Availability Zone gagal, Anda masih memiliki enam yang tersisa dan dapat terus melayani lalu lintas pelanggan Anda tanpa perlu menyediakan dan mengonfigurasi instance baru selama kegagalan. Mencapai stabilitas statis untuk EC2 kapasitas Anda memiliki biaya tambahan, karena, dalam hal ini, Anda menjalankan 50% instance tambahan. Tidak semua layanan di mana Anda dapat menyediakan sumber daya pra-penyediaan akan dikenakan biaya tambahan, seperti pra-penyediaan bucket S3 atau pengguna. Anda perlu mempertimbangkan setiap trade-off penerapan stabilitas statis terhadap risiko melebihi waktu pemulihan yang diinginkan untuk beban kerja Anda.

AWS Local Zones dan Outposts membawa bidang data AWS layanan tertentu lebih dekat ke pengguna akhir. Pesawat kontrol untuk layanan ini berada di Wilayah induk. Instans Local Zone atau Outposts Anda akan memiliki dependensi bidang kontrol untuk layanan zona seperti EC2 dan EBS pada Availability Zone tempat Anda membuat subnet Local Zone atau Outposts. Mereka juga akan memiliki dependensi pada pesawat kontrol Regional untuk layanan Regional seperti Elastic

Load Balancing ELB (), grup keamanan, dan pesawat kontrol Kubernetes yang dikelola Amazon Elastic Kubernetes Service EKS (Amazon) (jika Anda menggunakan). EKS Untuk informasi tambahan khusus untuk Outposts, lihat dokumentasi dan dukungan dan pemeliharaan. FAQ Menerapkan stabilitas statis saat menggunakan Local Zones atau Outposts untuk membantu meningkatkan ketahanan untuk mengontrol gangguan atau gangguan pesawat dalam konektivitas jaringan ke Wilayah induk.

Layanan regional

Layanan regional adalah layanan yang AWS telah dibangun di atas beberapa Availability Zone sehingga pelanggan tidak perlu mencari cara untuk memanfaatkan layanan zona dengan sebaik-baiknya. Kami secara logis mengelompokkan layanan yang diterapkan di beberapa Availability Zone untuk menyajikan satu titik akhir Regional kepada pelanggan. Amazon SQS dan Amazon DynamoDB adalah contoh layanan Regional. Mereka menggunakan independensi dan redundansi Availability Zone untuk meminimalkan kegagalan infrastruktur sebagai kategori risiko ketersediaan dan daya tahan. Amazon S3, misalnya, menyebarkan permintaan dan data di beberapa Availability Zone dan dirancang untuk memulihkan secara otomatis dari kegagalan Availability Zone. Namun, Anda hanya berinteraksi dengan titik akhir Regional layanan.

AWS percaya bahwa sebagian besar pelanggan dapat mencapai tujuan ketahanan mereka di satu Wilayah dengan menggunakan layanan Regional atau arsitektur Multi-AZ yang mengandalkan layanan zona. Namun, beberapa beban kerja mungkin memerlukan redundansi tambahan, dan Anda dapat menggunakan isolasi Wilayah AWS untuk membuat arsitektur Multi-Region untuk HA atau tujuan kontinuitas bisnis. Pemisahan fisik dan logis antara Wilayah AWS menghindari kegagalan yang berkorelasi di antara mereka. Dengan kata lain, mirip dengan jika Anda adalah EC2 pelanggan dan bisa mendapatkan keuntungan dari isolasi Availability Zone dengan menyebarkan di seluruh mereka, Anda bisa mendapatkan manfaat yang sama untuk layanan Regional dengan menyebarkan di beberapa Wilayah. Ini mengharuskan Anda menerapkan arsitektur Multi-wilayah untuk aplikasi Anda, yang dapat membantu Anda tahan terhadap gangguan layanan Regional.

Namun, mencapai manfaat arsitektur Multi-Region bisa jadi sulit; itu membutuhkan kerja yang cermat untuk memanfaatkan isolasi Regional sambil tidak membatalkan apa pun di tingkat aplikasi. Misalnya, jika Anda gagal dalam aplikasi antar Wilayah, Anda perlu menjaga pemisahan yang ketat antara tumpukan aplikasi di setiap Wilayah, mengetahui semua dependensi aplikasi, dan failover semua bagian aplikasi secara bersamaan. Mencapai hal ini dengan arsitektur berbasis layanan mikro yang kompleks yang memiliki banyak ketergantungan antar aplikasi memerlukan perencanaan dan koordinasi di antara banyak tim teknik dan bisnis. Mengizinkan beban kerja individu untuk

membuat keputusan failover mereka sendiri membuat koordinasi menjadi kurang kompleks, tetapi memperkenalkan perilaku modal melalui perbedaan signifikan dalam latensi yang terjadi di seluruh Wilayah dibandingkan dengan di dalam satu Wilayah.

AWS tidak menyediakan fitur replikasi Lintas Wilayah sinkron saat ini. Saat menggunakan datastore yang direplikasi secara asinkron (disediakan oleh AWS) di seluruh Wilayah, ada kemungkinan kehilangan atau ketidakkonsistenan data saat Anda gagal dalam aplikasi antar Wilayah. Untuk mengurangi kemungkinan ketidakkonsistenan, Anda memerlukan proses rekonsiliasi data yang andal yang Anda yakini dan mungkin perlu beroperasi pada beberapa penyimpanan data di seluruh portofolio beban kerja Anda, atau Anda harus bersedia menerima kehilangan data. Akhirnya, Anda perlu mempraktikkan failover untuk mengetahui bahwa itu akan berfungsi saat Anda membutuhkannya. Memutar aplikasi Anda secara teratur antar Wilayah untuk mempraktikkan failover adalah investasi waktu dan sumber daya yang substansif. Jika Anda memutuskan untuk menggunakan datastore yang direplikasi secara sinkron di seluruh Wilayah untuk mendukung aplikasi Anda yang berjalan dari lebih dari satu Wilayah secara bersamaan, karakteristik kinerja dan latensi database semacam itu yang mencakup 100-an atau 1000-an mil sangat berbeda dari database yang beroperasi di satu Wilayah. Ini mengharuskan Anda untuk merencanakan tumpukan aplikasi Anda dari bawah ke atas untuk memperhitungkan perilaku ini. Ini juga membuat ketersediaan kedua Wilayah menjadi ketergantungan yang sulit, yang dapat mengakibatkan penurunan ketahanan beban kerja Anda.

Layanan global

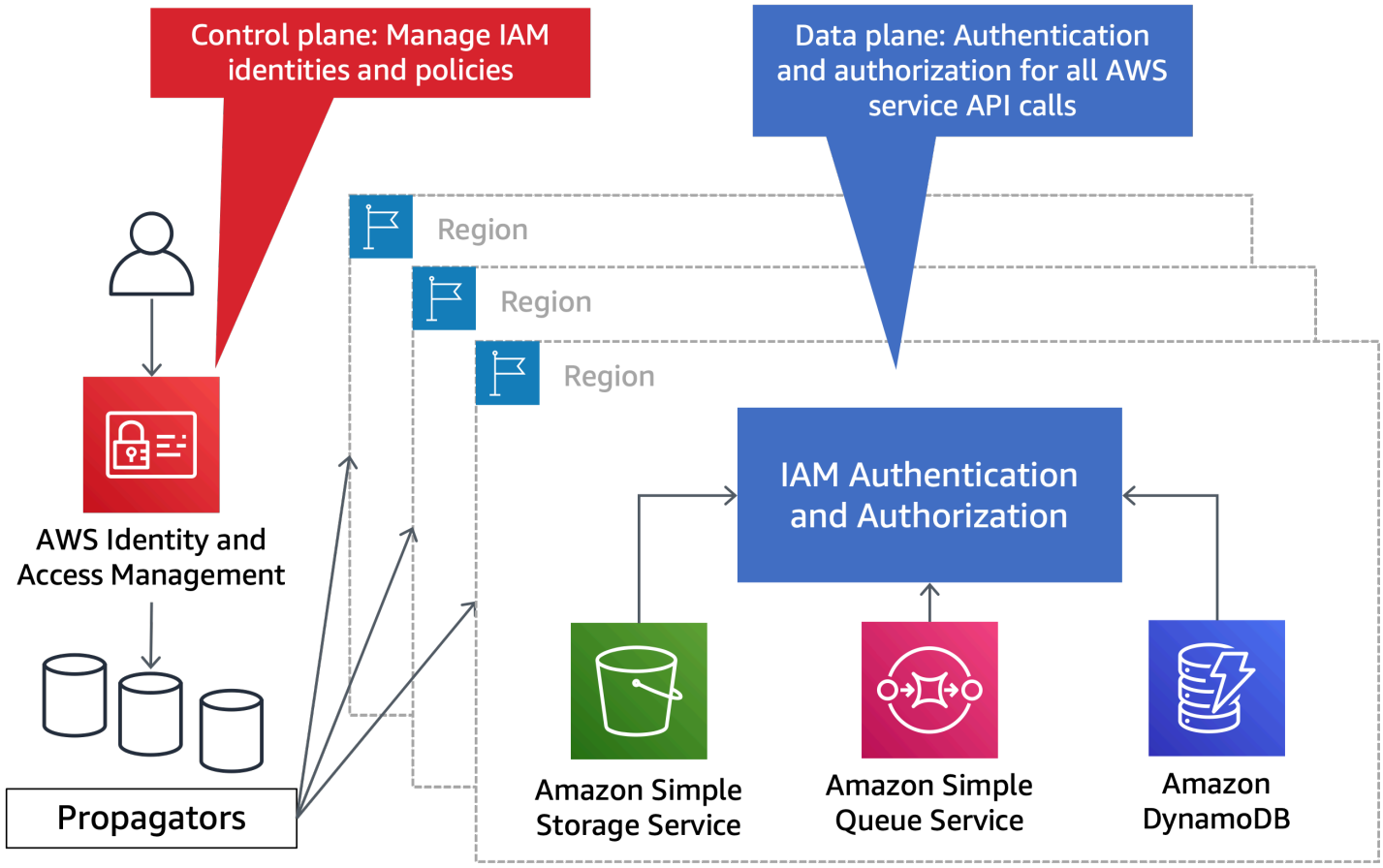
Selain AWS layanan Regional dan zona, ada satu set kecil AWS layanan yang pesawat kontrol dan pesawat datanya tidak ada secara independen di setiap Wilayah. Karena sumber daya mereka tidak spesifik Wilayah, mereka biasanya disebut sebagai global. AWS Layanan global masih mengikuti pola AWS desain konvensional untuk memisahkan bidang kontrol dan bidang data untuk mencapai stabilitas statis. Perbedaan signifikan untuk sebagian besar layanan global adalah bahwa pesawat kontrol mereka di-host dalam satu Wilayah AWS, sementara pesawat data mereka didistribusikan secara global. Ada tiga jenis layanan global dan satu set layanan yang dapat tampak global berdasarkan konfigurasi yang Anda pilih.

Bagian berikut akan mengidentifikasi setiap jenis layanan global dan bagaimana bidang kontrol dan bidang data mereka dipisahkan. Anda dapat menggunakan informasi ini untuk memandu bagaimana Anda membangun mekanisme ketersediaan tinggi (HA) dan pemulihan bencana (DR) yang andal tanpa perlu bergantung pada pesawat kontrol layanan global. Pendekatan ini membantu menghilangkan satu titik kegagalan dalam arsitektur Anda dan menghindari potensi dampak lintas

wilayah, bahkan ketika Anda beroperasi di Wilayah yang berbeda dari tempat pesawat kontrol layanan global di-host. Ini juga membantu Anda menerapkan mekanisme failover dengan aman yang tidak bergantung pada pesawat kontrol layanan global.

Layanan global yang unik berdasarkan partisi

Beberapa AWS layanan global ada di setiap partisi (disebut dalam paper ini sebagai layanan partisi). Layanan partisi menyediakan bidang kontrol mereka dalam satu Wilayah AWS. Beberapa layanan partisi, seperti AWS Network Manager, hanya mengontrol pesawat dan mengatur bidang data layanan lain. Layanan partisi lainnya, sepertiIAM, memiliki bidang data mereka sendiri yang diisolasi dan didistribusikan di semua partisi. Wilayah AWS Kegagalan dalam layanan partisi tidak memengaruhi partisi lain. Di `aws` partisi, bidang kontrol IAM layanan berada di `us-east-1` Wilayah, dengan bidang data terisolasi di setiap Wilayah partisi. Layanan partisi juga memiliki bidang kontrol independen dan pesawat data di `aws-us-gov` dan `aws-cn` partisi. Pemisahan bidang kontrol dan bidang data untuk IAM ditunjukkan pada diagram berikut.



IAMmemiliki bidang kontrol tunggal dan bidang data regional

Berikut ini adalah layanan partisi dan lokasi bidang kontrol mereka di `aws` partisi:

- AWS IAM (`us-east-1`)
- AWS Organizations (`us-east-1`)
- AWS Manajemen Akun (`us-east-1`)
- Route 53 Application Recovery Controller (ARC`us-west-2`) () - Layanan ini hanya ada di `aws` partisi
- AWS Manajer Jaringan (`us-west-2`)
- Rute 53 Pribadi DNS (`us-east-1`)

Jika salah satu dari pesawat kontrol layanan ini memiliki peristiwa yang berdampak pada ketersediaan, Anda mungkin tidak dapat menggunakan operasi CRUDL tipe -yang disediakan oleh layanan ini. Jadi, jika strategi pemulihan Anda memiliki ketergantungan pada operasi ini, dampak ketersediaan pada pesawat kontrol atau Wilayah yang menampung pesawat kontrol akan mengurangi peluang Anda untuk pemulihan yang berhasil. Lampiran A - Panduan layanan partisimenyediakan strategi untuk menghilangkan dependensi pada pesawat kontrol layanan global selama pemulihan.

> **Rekomendasi**
>
> Jangan mengandalkan bidang kontrol layanan partisi di jalur pemulihan Anda. Sebaliknya, andalkan operasi pesawat data dari layanan ini. Lihat Lampiran A - Panduan layanan partisi untuk detail tambahan tentang bagaimana Anda harus merancang untuk layanan partisi.

Layanan global di jaringan edge

Rangkaian AWS layanan global berikutnya memiliki bidang kontrol di `aws` partisi dan meng-host pesawat data mereka di infrastruktur titik kehadiran global (PoP) (dan berpotensi Wilayah AWS juga). Pesawat data yang di-host PoPs dapat diakses dari sumber daya di partisi apa pun serta internet. Misalnya, Route 53 mengoperasikan pesawat kontrolnya di `us-east-1` Wilayah, tetapi pesawat datanya didistribusikan di ratusan PoPs secara global, serta masing-masing Wilayah AWS (untuk mendukung Rute 53 Publik dan Swasta di DNS dalam Wilayah). Pemeriksaan kesehatan Route 53 juga merupakan bagian dari bidang data, dan dilakukan dari delapan Wilayah AWS di `aws` partisi. Klien dapat menyelesaikan DNS menggunakan zona yang dihosting publik Route 53 dari mana saja di internet, termasuk partisi lain seperti GovCloud, serta dari AWS Virtual Private Cloud (VPC). Berikut ini adalah layanan jaringan edge global dan lokasi bidang kontrolnya di `aws` partisi:

- Rute 53 Publik DNS (`us-east-1`)
- Amazon CloudFront (`us-east-1`)
- AWS WAF Klasik untuk CloudFront (`us-east-1`)
- AWS WAF untuk CloudFront (`us-east-1`)
- Amazon Certificate Manager (ACM) untuk CloudFront (`us-east-1`)
- AWSAkselerator Global (AGA) (`us-west-2`)
- AWS Shield Advanced (`us-east-1`)

Jika Anda menggunakan pemeriksaan AGA kesehatan untuk EC2 instance atau alamat IP Elastis, ini menggunakan pemeriksaan kesehatan Route 53. Membuat atau memperbarui pemeriksaan AGA kesehatan akan tergantung pada bidang kontrol Route 53 di`us-east-1`. Pelaksanaan pemeriksaan AGA kesehatan menggunakan pesawat data pemeriksaan kesehatan Rute 53.

Selama kegagalan yang berdampak pada Wilayah yang menampung pesawat kontrol untuk layanan ini, atau kegagalan yang berdampak pada bidang kontrol itu sendiri, Anda mungkin tidak dapat menggunakan operasi CRUDL tipe -yang disediakan oleh layanan ini. Jika Anda telah mengambil ketergantungan pada operasi ini dalam strategi pemulihan Anda, strategi itu mungkin lebih kecil kemungkinannya untuk berhasil daripada jika Anda hanya mengandalkan bidang data dari layanan ini.

> **Rekomendasi**
>
> Jangan mengandalkan bidang kontrol layanan jaringan tepi di jalur pemulihan Anda. Sebaliknya, andalkan operasi pesawat data dari layanan ini. Lihat Lampiran B - Panduan layanan global jaringan Edge untuk detail tambahan tentang cara merancang layanan global di jaringan edge.

Operasi Wilayah Tunggal Global

Kategori terakhir terdiri dari operasi pesawat kontrol khusus dalam layanan yang memiliki cakupan dampak global, bukan seluruh layanan seperti kategori sebelumnya. Saat Anda berinteraksi dengan layanan zona dan Regional di Wilayah yang Anda tentukan, operasi tertentu memiliki ketergantungan mendasar pada satu Wilayah yang berbeda dari tempat sumber daya berada. Ini berbeda dari layanan yang hanya disediakan di satu Wilayah; lihat Lampiran C - Layanan Single-Region untuk daftar layanan tersebut.

Selama kegagalan yang memengaruhi ketergantungan global yang mendasarinya, Anda mungkin tidak dapat menggunakan tindakan CRUDL -type dari operasi dependen. Jika Anda telah mengambil ketergantungan pada operasi ini dalam strategi pemulihan Anda, strategi itu mungkin lebih kecil kemungkinannya untuk berhasil daripada jika Anda hanya mengandalkan bidang data dari layanan ini. Anda harus menghindari ketergantungan pada operasi ini untuk strategi pemulihan Anda.

Berikut ini adalah daftar layanan yang mungkin bergantung pada layanan lain, yang memiliki cakupan global:

- Rute 53

  Beberapa AWS layanan membuat sumber daya yang menyediakan DNS nama khusus sumber daya. Misalnya, saat Anda menyediakan Elastic Load Balancer (ELB), layanan akan membuat DNS catatan publik dan pemeriksaan kesehatan di Route 53 untuk. ELB Ini bergantung pada pesawat kontrol Route 53 di`us-east-1`. Layanan lain yang Anda gunakan mungkin juga perlu menyediakanELB, membuat DNS catatan Route 53 publik, atau membuat pemeriksaan kesehatan Route 53 sebagai bagian dari alur kerja bidang kontrol mereka. Misalnya, penyediaan REST API sumber daya Amazon API Gateway, database Amazon Relational Database Service (AmazonRDS), atau domain OpenSearch Layanan Amazon semuanya menghasilkan pembuatan DNS catatan di Route 53. Berikut ini adalah daftar layanan yang bidang kontrolnya bergantung pada bidang kontrol Route 53 `us-east-1` untuk membuat, memperbarui, atau menghapus DNS catatan, zona yang dihosting, dan/atau membuat pemeriksaan kesehatan Route 53. Daftar ini tidak lengkap; ini dimaksudkan untuk menyoroti beberapa layanan yang paling umum digunakan yang tindakan bidang kontrolnya untuk membuat, memperbarui, atau menghapus sumber daya bergantung pada bidang kontrol Route 53:

  - Amazon API Gateway REST dan HTTP APIs
  - RDSContoh Amazon
  - Basis data Amazon Aurora
  - Penyeimbang ELB beban Amazon
  - Titik akhir AWS PrivateLink VPC
  - AWS Lambda URLs
  - Amazon ElastiCache
  - OpenSearch Layanan Amazon
  - Amazon CloudFront
  - Amazon MemoryDB

- Amazon Neptune
- Akselerator Amazon DynamoDB () DAX
- AGA
- Amazon Elastic Container Service (AmazonECS) dengan Service Discovery DNS berbasis (yang menggunakan AWS Cloud Map API untuk mengelola Route 53DNS)
- Pesawat kontrol Amazon EKS Kubernetes

  Penting untuk dicatat bahwa VPC DNS layanan EC2misalnya nama host ada secara independen di masing-masing Wilayah AWS dan tidak bergantung pada bidang kontrol Route 53. Catatan yang AWS dibuat untuk EC2 instance dalam VPC DNS layanan, seperti,`ip-10-0-10.ec2.internal`,`ip-10-0-1-5.compute.us-west-2.compute.internal`, dan `i-0123456789abcdef.ec2.internali-0123456789abcdef.us-west-2.compute.internal`, tidak bergantung pada bidang kontrol Route 53 di`us-east-1`.

  > **Rekomendasi**
  >
  > Jangan mengandalkan pembuatan, pembaruan, atau penghapusan sumber daya yang memerlukan pembuatan, pembaruan, atau penghapusan catatan sumber daya Route 53, zona yang dihosting, atau pemeriksaan kesehatan di jalur pemulihan Anda. Pra-penyediaan sumber daya ini, sepertiELBs, untuk mencegah ketergantungan pada bidang kontrol Route 53 di jalur pemulihan Anda.

- Amazon S3

  Operasi bidang kontrol Amazon S3 berikut memiliki ketergantungan mendasar `us-east-1` pada partisi. `aws` Kegagalan yang memengaruhi Amazon S3 atau layanan `us-east-1` lain dapat menyebabkan tindakan pesawat kontrol ini terganggu di Wilayah lain:

```
PutBucketCors
DeleteBucketCors
PutAccelerateConfiguration
PutBucketRequestPayment
PutBucketObjectLockConfiguration
PutBucketTagging
DeleteBucketTagging
```

```
PutBucketReplication
DeleteBucketReplication
PutBucketEncryption
DeleteBucketEncryption
PutBucketLifecycle
DeleteBucketLifecycle
PutBucketNotification
PutBucketLogging
DeleteBucketLogging
PutBucketVersioning
PutBucketPolicy
DeleteBucketPolicy
PutBucketOwnershipControls
DeleteBucketOwnershipControls
PutBucketAcl
PutBucketPublicAccessBlock
DeleteBucketPublicAccessBlock
```

Bidang kontrol untuk Amazon S3 Multi-Region Access Points (MRAP) hanya di-host `us-west-2` dan meminta untuk membuat, memperbarui, atau menghapus MRAPs target Wilayah tersebut secara langsung. Bidang kontrol untuk MRAP juga memiliki dependensi mendasar pada AGA in`us-west-2`, Route 53 in`us-east-1`, dan ACM di setiap Wilayah tempat MRAP dikonfigurasi untuk menyajikan konten. Anda tidak boleh bergantung pada ketersediaan pesawat MRAP kontrol di jalur pemulihan Anda atau di pesawat data sistem Anda sendiri. Ini berbeda dari kontrol MRAP failover yang digunakan untuk menentukan status perutean aktif atau pasif untuk setiap bucket Anda di. MRAP Ini APIs di-host dalam lima Wilayah AWS dan dapat digunakan untuk secara efektif mengalihkan lalu lintas menggunakan pesawat data layanan.

Selain itu, nama bucket Amazon S3 unik secara global dan semua panggilan ke `CreateBucket` dan `DeleteBucket` APIs bergantung pada`us-east-1`, di `aws` partisi, untuk memastikan keunikan nama, meskipun API panggilan diarahkan ke Wilayah tertentu tempat Anda ingin membuat bucket. Terakhir, jika Anda memiliki alur kerja pembuatan bucket yang penting, Anda tidak boleh bergantung pada ketersediaan ejaan tertentu dari nama bucket, terutama yang mengikuti pola yang terlihat.

> **Rekomendasi**
>
> Jangan mengandalkan menghapus atau membuat bucket S3 baru atau memperbarui konfigurasi bucket S3 sebagai bagian dari jalur pemulihan Anda. Pra-penyediaan semua bucket S3 yang diperlukan dengan konfigurasi yang diperlukan sehingga Anda tidak

perlu melakukan perubahan untuk pulih dari kegagalan. Pendekatan ini juga berlaku untukMRAPs.

- CloudFront

  Amazon API Gateway menyediakan titik akhir yang dioptimalkan tepi API. Membuat titik akhir ini bergantung pada bidang CloudFront kontrol `us-east-1` untuk membuat distribusi di depan titik akhir gateway.

  > **Rekomendasi**
  >
  > Jangan mengandalkan pembuatan titik akhir API Gateway baru yang dioptimalkan tepi sebagai bagian dari jalur pemulihan Anda. Pra-penyediaan semua titik akhir API Gateway yang diperlukan.

  Semua dependensi yang dibahas di bagian ini adalah tindakan bidang kontrol, bukan tindakan bidang data. Jika beban kerja Anda dikonfigurasi agar stabil secara statis, dependensi ini seharusnya tidak memengaruhi jalur pemulihan Anda, dengan mengingat bahwa stabilitas statis memerlukan pekerjaan atau layanan tambahan untuk diterapkan.

Layanan yang menggunakan endpoint global default

Dalam beberapa kasus, AWS layanan menyediakan titik akhir global default, seperti AWS Security Token Service (AWS STS). Layanan lain mungkin menggunakan titik akhir global default ini dalam konfigurasi defaultnya. Ini berarti bahwa layanan Regional yang Anda gunakan dapat memiliki ketergantungan global pada satu Wilayah AWS. Rincian berikut menjelaskan cara menghapus dependensi yang tidak diinginkan pada endpoint global default yang akan membantu Anda menggunakan layanan dengan cara Regional.

AWS STS: STS adalah layanan web yang memungkinkan Anda untuk meminta kredensi hak istimewa terbatas sementara untuk IAM pengguna atau untuk pengguna yang Anda autentikasi (pengguna gabungan). STSpenggunaan dari kit pengembangan AWS perangkat lunak (SDK) dan antarmuka baris perintah (CLI) default ke. `us-east-1` STSLayanan ini juga menyediakan titik akhir Regional. Titik akhir ini diaktifkan secara default di Wilayah yang juga diaktifkan secara default. Anda dapat memanfaatkan ini kapan saja dengan mengonfigurasi SDK atau CLI mengikuti petunjuk

berikut: Titik akhir AWS STSregional. Menggunakan Sigv4a juga memerlukan kredensil sementara yang diminta dari titik akhir Regional. STS Anda tidak dapat menggunakan STS titik akhir global untuk operasi ini.

> **Rekomendasi**
>
> Perbarui CLI konfigurasi SDK dan Anda untuk menggunakan STS titik akhir Regional.

Security Assertion Markup Language (SAML) Masuk: SAML layanan ada di semua. Wilayah AWS Untuk menggunakan layanan ini, pilih SAML titik akhir regional yang sesuai, seperti https://us-west-2.signin.aws.amazon.com/saml. Anda harus memperbarui konfigurasi dalam kebijakan kepercayaan dan Penyedia Identitas (iDP) Anda untuk menggunakan titik akhir regional. Lihat AWS SAMLdokumentasi untuk detail spesifik.

Jika Anda menggunakan IDP yang juga di-host AWS, ada risiko bahwa mereka juga dapat terpengaruh selama peristiwa AWS kegagalan. Hal ini dapat mengakibatkan Anda tidak dapat memperbarui konfigurasi IDP Anda atau Anda mungkin tidak dapat melakukan federasi sepenuhnya. Anda harus menyediakan terlebih dahulu pengguna “break-glass” jika IDP Anda rusak atau tidak tersedia. Lihat detail tentang cara membuat pengguna break-glass dengan cara yang stabil secara statis. Lampiran A - Panduan layanan partisi

> **Rekomendasi**
>
> Perbarui kebijakan kepercayaan IAM peran Anda untuk menerima SAML login dari beberapa Wilayah. Selama kegagalan, perbarui konfigurasi IDP Anda untuk menggunakan SAML titik akhir Regional yang berbeda jika titik akhir pilihan Anda terganggu. Buat pengguna break-glass jika IDP Anda rusak atau tidak tersedia.

AWS IAMPusat Identitas: Identity Center adalah layanan berbasis cloud yang memudahkan pengelolaan akses masuk tunggal ke aplikasi pelanggan dan cloud secara terpusat. Akun AWS Pusat Identitas harus digunakan di satu Wilayah pilihan Anda. Namun, perilaku default untuk layanan ini adalah menggunakan SAML titik akhir global (https://signin.aws.amazon.com/saml), yang di-host `dius-east-1`. Jika Anda telah menerapkan Pusat Identitas ke dalam yang berbeda Wilayah AWS, Anda harus memperbarui status relai URL dari setiap izin yang ditetapkan untuk menargetkan titik akhir konsol Regional yang sama dengan penerapan Pusat Identitas Anda. Misalnya, jika Anda menerapkan Pusat Identitas ke dalam`us-west-2`, Anda harus memperbarui status relaystate dari

set izin Anda untuk menggunakan https://us-west-2.console.aws.amazon.com. Ini akan menghapus ketergantungan apa pun `us-east-1` dari penyebaran Pusat Identitas Anda.

Selain itu, karena Pusat IAM Identitas hanya dapat diterapkan ke dalam satu Wilayah, Anda harus menyediakan pengguna “break-glass” terlebih dahulu jika penerapan Anda terganggu. Lihat detail tentang cara membuat pengguna break-glass dengan cara yang stabil secara statis. Lampiran A - Panduan layanan partisi

> **Rekomendasi**
>
> Setel status relaystate URL dari set izin Anda di Pusat IAM Identitas agar sesuai dengan Wilayah tempat Anda memiliki layanan yang digunakan. Buat pengguna break-glass jika penyebaran Pusat IAM Identitas Anda tidak tersedia.

Lensa Penyimpanan Amazon S3: Lensa Penyimpanan menyediakan dasbor default yang disebut. default-account-dashboard Konfigurasi dasbor dan metrik terkait disimpan di`us-east-1`. Anda dapat membuat dasbor tambahan di Wilayah lain dengan menentukan Wilayah beranda untuk konfigurasi dasbor dan data metrik.

> **Rekomendasi**
>
> Jika Anda memerlukan data dari dasbor Lensa Penyimpanan S3 default selama kegagalan yang memengaruhi layanan`us-east-1`, buat dasbor tambahan di Wilayah rumah alternatif. Anda juga dapat menduplikasi dasbor khusus lainnya yang telah Anda buat di Wilayah tambahan.

Ringkasan layanan global

Pesawat data untuk layanan global menerapkan prinsip isolasi dan independensi yang serupa dengan AWS layanan Regional. Kegagalan yang memengaruhi bidang data IAM di Wilayah tidak memengaruhi pengoperasian bidang IAM data di wilayah lain Wilayah AWS. Demikian pula, kegagalan yang memengaruhi bidang data Route 53 di PoP tidak memengaruhi pengoperasian bidang data Route 53 di bagian PoPs lainnya. Oleh karena itu, yang harus kita pertimbangkan adalah peristiwa ketersediaan layanan yang mempengaruhi Wilayah tempat pesawat kontrol beroperasi atau mempengaruhi bidang kontrol itu sendiri. Karena hanya ada satu bidang kontrol untuk setiap layanan global, kegagalan yang mempengaruhi bidang kontrol itu dapat memiliki efek lintas wilayah

pada operasi CRUDL -type (yang merupakan operasi konfigurasi yang biasanya digunakan untuk mengatur atau mengkonfigurasi layanan sebagai lawan dari penggunaan langsung layanan).

Cara paling efektif untuk merancang beban kerja untuk menggunakan layanan global secara tangguh adalah dengan menggunakan stabilitas statis. Selama skenario kegagalan, rancang beban kerja Anda agar tidak perlu melakukan perubahan dengan bidang kontrol untuk mengurangi dampak atau kegagalan ke lokasi yang berbeda. Lihat Lampiran A - Panduan layanan partisi dan Lampiran B - Panduan layanan global jaringan Edge untuk panduan preskriptif tentang cara memanfaatkan jenis layanan global ini untuk menghilangkan dependensi bidang kontrol dan menghilangkan satu titik kegagalan. Jika Anda memerlukan data dari operasi bidang kontrol untuk pemulihan, cache data ini di penyimpanan data yang dapat diakses melalui bidang datanya, seperti parameter AWS Systems Manager Parameter Store (SSMParameter Store), tabel DynamoDB, atau bucket S3. Untuk redundansi, Anda juga dapat memilih untuk menyimpan data tersebut di Wilayah tambahan. Misalnya, mengikuti praktik terbaik untuk Route 53 Application Recovery Controller (ARC), Anda harus membuat hardcode atau menandai lima titik akhir cluster Regional Anda. Selama peristiwa kegagalan, Anda mungkin tidak dapat mengakses beberapa API operasi, termasuk operasi Route 53 ARC API yang tidak dihosting di cluster pesawat data yang sangat andal. Anda dapat membuat daftar titik akhir untuk ARC cluster Route 53 Anda dengan menggunakan operasi. `DescribeCluster` API

Berikut ini adalah ringkasan dari beberapa kesalahan konfigurasi atau anti-pola yang paling umum yang memperkenalkan dependensi pada bidang kontrol layanan global:

- Membuat perubahan pada rekaman Route 53, seperti memperbarui nilai catatan A atau mengubah bobot set rekaman tertimbang, untuk melakukan failover.
- Membuat atau memperbarui IAM sumber daya, termasuk IAM peran dan kebijakan, selama kegagalan. Ini biasanya tidak disengaja, tetapi mungkin merupakan hasil dari rencana failover yang belum teruji.
- Mengandalkan Pusat IAM Identitas bagi operator untuk mendapatkan akses ke lingkungan produksi selama peristiwa kegagalan.
- Mengandalkan konfigurasi Pusat IAM Identitas default untuk memanfaatkan konsol `us-east-1` saat Anda telah menerapkan Pusat Identitas ke Wilayah lain.
- Membuat perubahan pada bobot panggilan AGA lalu lintas untuk melakukan failover Regional secara manual.
- Memperbarui konfigurasi asal CloudFront distribusi agar gagal menjauh dari asal yang terganggu.
- Penyediaan sumber daya pemulihan bencana (DR), suka ELBs dan RDS contoh selama peristiwa kegagalan, yang bergantung pada pembuatan DNS catatan di Route 53.

Berikut ini adalah ringkasan dari rekomendasi yang diberikan di bagian ini untuk menggunakan layanan global dengan cara yang tangguh yang akan membantu mencegah anti-pola umum sebelumnya.

Ringkasan rekomendasi

Jangan mengandalkan bidang kontrol layanan partisi di jalur pemulihan Anda. Sebaliknya, andalkan operasi pesawat data dari layanan ini. Lihat Lampiran A - Panduan layanan partisi untuk detail tambahan tentang bagaimana Anda harus merancang untuk layanan partisi.
Jangan mengandalkan bidang kontrol layanan jaringan tepi di jalur pemulihan Anda. Sebaliknya, andalkan operasi pesawat data dari layanan ini. Lihat Lampiran B - Panduan layanan global jaringan Edge untuk detail tambahan tentang cara merancang layanan global di jaringan edge.
Jangan mengandalkan pembuatan, pembaruan, atau penghapusan sumber daya yang memerlukan pembuatan, pembaruan, atau penghapusan catatan sumber daya Route 53, zona yang dihosting, atau pemeriksaan kesehatan di jalur pemulihan Anda. Pra-penyediaan sumber daya ini, sepertiELBs, untuk mencegah ketergantungan pada bidang kontrol Route 53 di jalur pemulihan Anda.
Jangan mengandalkan menghapus atau membuat bucket S3 baru atau memperbarui konfigurasi bucket S3 sebagai bagian dari jalur pemulihan Anda. Pra-penyediaan semua bucket S3 yang diperlukan dengan konfigurasi yang diperlukan sehingga Anda tidak perlu melakukan perubahan untuk pulih dari kegagalan. Pendekatan ini juga berlaku untukMRAPs.
Jangan mengandalkan pembuatan titik akhir API Gateway baru yang dioptimalkan tepi sebagai bagian dari jalur pemulihan Anda. Pra-penyediaan semua titik akhir API Gateway yang diperlukan.
Perbarui CLI konfigurasi SDK dan Anda untuk menggunakan STS titik akhir Regional.
Perbarui kebijakan kepercayaan IAM peran Anda untuk menerima SAML login dari beberapa Wilayah. Selama kegagalan, perbarui konfigurasi IDP Anda untuk menggunakan SAML titik akhir Regional yang berbeda jika titik akhir pilihan Anda terganggu. Buat pengguna break-glass jika IDP Anda rusak atau tidak tersedia.
Setel status relaystate URL dari set izin Anda di Pusat IAM Identitas agar sesuai dengan Wilayah tempat Anda memiliki layanan yang digunakan. Buat pengguna break-glass jika penyebaran Pusat Identitas Anda tidak tersedia.
Jika Anda memerlukan data dari dasbor Lensa Penyimpanan S3 default selama kegagalan yang memengaruhi layanan`us-east-1`, buat dasbor tambahan di Wilayah rumah alternatif.

Anda juga dapat menduplikasi dasbor khusus lainnya yang telah Anda buat di Wilayah tambahan.

Kesimpulan

AWSmenyediakan beberapa konstruksi yang berbeda untuk batas isolasi kesalahan. Anda harus mempertimbangkan bagaimana Anda membuat arsitek untuk layanan zonal, Regional, dan global serta potensi dampak pada beban kerja Anda dan kemampuan beban kerja Anda untuk pulih selama gangguan bidang kontrol. Stabilitas statis adalah salah satu cara utama agar Anda dapat menghindari dependensi bidang kontrol dan menciptakan mekanisme HA dan DR yang andal dan tangguh saat Anda menggunakan layanan. AWS

Lampiran A - Panduan layanan partisi

Untuk layanan partisi, Anda harus menerapkan stabilitas statis untuk menjaga ketahanan beban kerja Anda selama gangguan bidang kontrol AWS layanan. Berikut ini memberikan panduan preskriptif tentang bagaimana mempertimbangkan dependensi pada layanan partisi serta apa yang akan dan mungkin tidak bekerja selama gangguan bidang kontrol.

AWS Identity and Access Management (IAM)

Bidang kontrol AWS Identity and Access Management (IAM) terdiri dari semua API IAM publik (termasuk Access Advisor tetapi tidak Access Analyzer atau IAM Roles Anywhere). Ini termasuk tindakan seperti`CreateRole`,`AttachRolePolicy`,`ChangePassword`,`UpdateSAMLProvider`, dan`UpdateLoginProfile`. Pesawat data IAM menyediakan otentikasi dan otorisasi untuk prinsipal IAM di masing-masing. Wilayah AWS Selama gangguan bidang kontrol, operasi tipe CRUDL untuk IAM mungkin tidak berfungsi, tetapi otentikasi dan otorisasi untuk prinsipal yang ada akan terus bekerja. STS adalah layanan data plane-only yang terpisah dari IAM, dan tidak tergantung pada bidang kontrol IAM.

Apa artinya ini adalah bahwa ketika Anda berencana untuk dependensi pada IAM, Anda tidak harus bergantung pada pesawat kontrol IAM di jalur pemulihan Anda. Misalnya, desain yang stabil secara statis untuk pengguna admin “break-glass” adalah membuat pengguna dengan izin yang sesuai terlampir, mengatur kata sandi dan kunci akses dan kunci akses rahasia yang disediakan, lalu mengunci kredensi tersebut di vault fisik atau virtual. Bila diperlukan selama keadaan darurat, ambil kredensi pengguna dari vault dan gunakan sesuai kebutuhan. non-statically-stableDesain akan menyediakan pengguna selama kegagalan, atau memiliki pengguna pra-penyediaan, tetapi hanya melampirkan kebijakan admin bila diperlukan. Pendekatan ini akan tergantung pada bidang kontrol IAM.

AWS Organizations

Pesawat AWS Organizations kontrol terdiri dari semua API Organizations publik seperti`AcceptHandshake`,`AttachPolicy`,`CreateAccount`,`CreatePolicy`, dan`ListAccounts`. Tidak ada pesawat data untukAWS Organizations. Ini mengatur pesawat data untuk layanan lain seperti IAM. Selama gangguan bidang kontrol, operasi tipe CRUDL untuk Organizations mungkin tidak berfungsi, tetapi kebijakan, seperti Kebijakan Kontrol Layanan (SCP) dan Kebijakan Tag, akan terus berfungsi dan dievaluasi sebagai bagian dari proses otorisasi IAM. Kemampuan admin yang

didelegasikan dan fitur multi-akun di AWS layanan lain yang didukung oleh Organizations juga akan terus bekerja.

Artinya, ketika Anda merencanakan dependensiAWS Organizations, Anda tidak boleh bergantung pada bidang kontrol Organizations di jalur pemulihan Anda. Sebagai gantinya, terapkan stabilitas statis dalam rencana pemulihan Anda. Misalnya, non-statically-stable pendekatan mungkin untuk memperbarui SCP untuk menghapus pembatasan yang diizinkan Wilayah AWS melalui `aws:RequestedRegion` kondisi, atau untuk mengaktifkan izin admin untuk peran IAM tertentu. Ini bergantung pada bidang kontrol Organizations untuk membuat pembaruan ini. Pendekatan yang lebih baik adalah dengan menggunakan tag sesi untuk memberikan penggunaan izin admin. Identity Provider (IdP) Anda dapat menyertakan tag sesi yang dapat dievaluasi terhadap `aws:PrincipalTag` kondisi, yang membantu Anda mengonfigurasi izin secara dinamis untuk prinsipal tertentu sambil membantu SCP Anda tetap statis. Ini menghilangkan dependensi pada bidang kontrol dan hanya menggunakan tindakan bidang data.

AWSManajemen Akun

Bidang kontrol Manajemen AWS Akun dihosting di us-timur-1 dan terdiri dari semua API publik untuk mengelolaAkun AWS, seperti dan. `GetContactInformation` `PutContactInformation` Ini juga termasuk membuat atau menutup yang baru Akun AWS melalui konsol manajemen. API untuk`CloseAccount`,, `CreateAccount``CreateGovCloudAccount`, dan `DescribeAccount` merupakan bagian dari AWS Organizations control plane, yang juga di-host di us-timur-1. Selain itu, membuat GovCloud akun di luar AWS Organizations bergantung pada bidang kontrol Akun AWS manajemen di us-timur-1. Selain itu, GovCloud akun harus 1:1 ditautkan ke Akun AWS dalam `aws` partisi. Membuat akun di `aws-cn` partisi tidak bergantung pada us-west-1. Pesawat data untuk Akun AWS adalah akun itu sendiri. Selama gangguan bidang kontrol, operasi tipe CRUDL (seperti membuat akun baru atau mendapatkan dan memperbarui informasi kontak) mungkin tidak berfungsi. Akun AWS Referensi ke akun dalam kebijakan IAM akan terus bekerja.

Artinya, ketika Anda merencanakan dependensi pada Manajemen AWS Akun, Anda tidak boleh mengandalkan bidang kontrol Manajemen Akun di jalur pemulihan Anda. Meskipun bidang kontrol Manajemen Akun tidak menyediakan fungsionalitas langsung yang biasanya Anda gunakan dalam situasi pemulihan, mungkin ada saat-saat ketika Anda melakukannya. Misalnya, desain statis-stabil akan pra-penyediaan semua yang Anda butuhkan untuk failover. Akun AWS non-statically-stableDesain akan membuat baru Akun AWS selama acara kegagalan untuk menjadi tuan rumah sumber daya DR Anda.

Pengendali Pemulihan Aplikasi Route 53

Bidang kontrol untuk Route 53 ARC terdiri dari API untuk kontrol pemulihan dan kesiapan pemulihan, seperti yang diidentifikasi di: Titik akhir dan kuota Amazon Route 53 Application Recovery Controller. Anda mengelola pemeriksaan kesiapan, kontrol routing, dan operasi cluster dengan menggunakan control plane. Bidang data ARC adalah klaster pemulihan Anda, yang mengelola nilai kontrol perutean yang ditanyakan oleh pemeriksaan kesehatan Route 53, dan juga menerapkan aturan keselamatan. Fungsionalitas bidang data Route 53 ARC diakses melalui API klaster pemulihan Anda seperti. `https://aaaaaaaa.route53-recovery-cluster.eu-west-1.amazonaws.com`

Artinya, Anda tidak boleh mengandalkan bidang kontrol Route 53 ARC di jalur pemulihan Anda. Ada dua praktik terbaik yang membantu menerapkan panduan ini:

- Pertama, bookmark atau kode keras lima titik akhir klaster Regional. Ini menghilangkan kebutuhan untuk menggunakan operasi DescribeCluster control plane selama skenario failover untuk menemukan nilai endpoint.
- Kedua, gunakan API klaster Route 53 ARC dengan menggunakan CLI atau SDK untuk melakukan pembaruan pada kontrol perutean dan bukan. Konsol Manajemen AWS Ini menghapus konsol manajemen sebagai dependensi untuk rencana failover Anda dan memastikan itu hanya bergantung pada tindakan bidang data.

AWSNetwork Manager

Layanan AWS Network Manager terutama merupakan sistem kontrol khusus pesawat yang dihosting di kami-barat-2. Tujuannya adalah untuk mengelola konfigurasi jaringan inti jaringan area AWS Cloud luas (WAN) Anda secara terpusat dan jaringan AWS Transit Gateway Anda di seluruhAkun AWS, Wilayah, dan lokasi lokal. Ini juga menggabungkan metrik Cloud WAN Anda di us-west-2, yang juga dapat diakses melalui bidang data. CloudWatch Jika Network Manager terganggu, bidang data dari layanan yang diaturnya tidak akan terpengaruh. CloudWatchMetrik untuk Cloud juga tersedia di us-west-2. Jika Anda ingin data metrik historis, seperti byte masuk dan keluar per Wilayah, untuk memahami seberapa banyak lalu lintas yang mungkin bergeser ke Wilayah lain selama kegagalan yang memengaruhi kami-barat-2, atau untuk tujuan operasional lainnya, Anda dapat mengekspor metrik tersebut sebagai data CSV langsung dari CloudWatch konsol atau menggunakan metode ini: Publikasikan metrik Amazon ke file CSV. CloudWatch Data dapat ditemukan di bawah `AWS/Network Manager` namespace dan Anda dapat melakukan ini pada jadwal yang Anda pilih dan menyimpannya di S3 atau di penyimpanan data lain yang Anda pilih. Untuk mengimplementasikan rencana pemulihan statis yang stabil, jangan gunakan AWS Network Manager untuk membuat

pembaruan ke jaringan Anda, atau mengandalkan data dari operasi bidang kontrol untuk input failover.

Rute 53 DNS Pribadi

Route 53 zona host pribadi didukung di setiap partisi; namun, pertimbangan untuk zona host pribadi dan zona host publik di Route 53 adalah sama. Lihat Amazon Route 53 dalam panduan layanan global jaringan Appendix B - Edge.

Lampiran B - Panduan layanan global jaringan Edge

Untuk layanan global jaringan edge, Anda harus menerapkan stabilitas statis untuk menjaga ketahanan beban kerja Anda selama gangguan bidang kontrol AWS layanan.

Route 53

Bidang kontrol Route 53 terdiri dari semua API publik Route 53 yang mencakup fungsionalitas untuk zona yang di-host, catatan kondisi, log kueri DNS, set delegasi yang dapat digunakan kembali, kebijakan lalu lintas, dan tanda alokasi biaya. Ini di-host di us-east-1. Pesawat data adalah layanan DNS otoritatif, yang berjalan di lebih dari 200 lokasi PoP serta di masing-masingWilayah AWS, menjawab pertanyaan DNS berdasarkan zona host dan data pemeriksaan kesehatan Anda. Selain itu, Route 53 memiliki bidang data untuk pemeriksaan kesehatan yang juga merupakan layanan yang didistribusikan secara global di beberapa. Wilayah AWS Pesawat data ini melakukan pemeriksaan kesehatan, agregat hasilnya, dan mengirimkannya ke pesawat data Route 53 DNS publik dan swasta dan AGA. Selama gangguan bidang kontrol, operasi tipe CRUDL untuk Route 53 mungkin tidak berfungsi, tetapi resolusi DNS dan pemeriksaan kesehatan, dan pembaruan perutean yang dihasilkan dari perubahan pemeriksaan kesehatan, akan terus berfungsi.

Apa artinya ini adalah bahwa ketika Anda merencanakan dependensi pada Route 53, Anda tidak boleh bergantung pada bidang kontrol Route 53 di jalur pemulihan Anda. Misalnya, desain yang stabil secara statis adalah menggunakan status pemeriksaan kesehatan untuk melakukan failover antar Wilayah atau untuk mengevakuasi Availability Zone. Anda dapat menggunakan kontrol perutean Route 53 Application Recovery Controller (ARC) untuk mengubah status pemeriksaan kesehatan secara manual dan mengubah respons terhadap kueri DNS. Ada pola yang mirip dengan apa yang ARC berikan yang dapat Anda terapkan berdasarkan kebutuhan Anda. Beberapa pola ini diuraikan dalam Membuat Mekanisme Pemulihan Bencana menggunakan Route 53 dan di bagian pemutus sirkuit pemeriksaan kesehatan Pola Ketahanan Multi-AZ Tingkat Lanjut. Jika Anda telah memilih untuk menggunakan paket DR Multi-Wilayah, pra-penyediaan sumber daya yang memerlukan data DNS untuk dibuat, seperti contoh ELB dan RDS. non-statically-stableDesain akan memperbarui nilai data sumber daya Route 53 melalui `ChangeResourceRecordSets` API, mengubah berat catatan tertimbang, atau membuat catatan baru untuk melakukan failover. Pendekatan ini bergantung pada bidang kontrol Route 53.

Amazon CloudFront

Pesawat CloudFront kontrol Amazon terdiri dari semua CloudFront API publik untuk mengelola distribusi, dan dihosting di us-timur-1. Pesawat data adalah distribusi itu sendiri dilayani dari jaringan PoPs di tepi. Ia melakukan penanganan permintaan, routing, dan caching konten asal Anda. Selama gangguan bidang kontrol, operasi tipe CRUDL untuk CloudFront (termasuk permintaan pembatalan) mungkin tidak berfungsi, tetapi konten Anda akan terus di-cache dan ditayangkan, dan failover asal akan terus berfungsi.

Apa artinya ini adalah bahwa ketika Anda berencana untuk dependensi padaCloudFront, Anda tidak harus bergantung pada bidang CloudFront kontrol di jalur pemulihan Anda. Misalnya, desain yang stabil secara statis adalah menggunakan failover asal otomatis untuk mengurangi dampak dari gangguan ke salah satu asal Anda. Anda juga dapat memilih untuk membuat penyeimbangan muatan asal atau failover menggunakan Lamda @Edge, lihat Tiga pola desain lanjutan untuk aplikasi tinggi yang tersedia menggunakan Amazon dan Menggunakan Amazon CloudFront CloudFront dan Amazon S3 untuk membangun aplikasi kedekatan geoaktif aktif multi-wilayah untuk detail selengkapnya tentang pola tersebut. non-statically-stableDesain akan secara manual memperbarui konfigurasi distribusi Anda dalam menanggapi kegagalan asal. Pendekatan ini akan tergantung pada bidang CloudFront kontrol.

Certificate Manager Amazon

Jika Anda menggunakan sertifikat kustom dengan CloudFront distribusi Anda, Anda juga memiliki ketergantungan pada ACM. Menggunakan sertifikat khusus dengan CloudFront distribusi Anda bergantung pada bidang kontrol ACM di Wilayah us-east-1. Selama gangguan bidang kontrol, sertifikat yang ada yang dikonfigurasi dalam distribusi Anda akan terus berfungsi serta perpanjangan sertifikat otomatis. Jangan mengandalkan mengubah konfigurasi distribusi atau membuat sertifikat baru sebagai bagian dari jalur pemulihan Anda.

AWSFirewall Aplikasi Web (WAF) dan WAF Classic

Jika Anda menggunakan AWS WAF CloudFront distribusi Anda, Anda memiliki ketergantungan pada bidang kontrol WAF, yang juga di-host di Wilayah us-timur-1. Selama gangguan bidang kontrol, daftar kontrol akses web (ACL) yang dikonfigurasi dan aturan terkait terus berfungsi. Jangan mengandalkan memperbarui ACL web WAF Anda sebagai bagian dari jalur pemulihan Anda.

AWSAkselerator Global Accelerator

Pesawat kontrol AGA terdiri dari semua API AGA publik dan dihosting di kami-barat-2. Pesawat data adalah perutean jaringan dari alamat IP anycast yang disediakan oleh AGA ke endpoint terdaftar Anda. AGA juga menggunakan pemeriksaan kesehatan Route 53 untuk menentukan kesehatan titik akhir AGA Anda, yang merupakan bagian dari pesawat data Route 53. Selama gangguan bidang kontrol, operasi tipe CRUDL untuk AGA mungkin tidak berfungsi. Perutean ke titik akhir yang ada, serta pemeriksaan kesehatan yang ada, panggilan lalu lintas, dan konfigurasi bobot titik akhir yang digunakan untuk merutekan atau mengalihkan lalu lintas ke titik akhir dan grup titik akhir lainnya, akan terus berfungsi.

Artinya, ketika Anda merencanakan ketergantungan pada AGA, Anda tidak boleh mengandalkan bidang kontrol AGA di jalur pemulihan Anda. Misalnya, desain yang stabil-statis adalah menggunakan status pemeriksaan kesehatan yang dikonfigurasi untuk gagal menjauh dari titik akhir yang tidak sehat. Lihat Deploying aplikasi multi-region dalam AWS menggunakan AWS Global Accelerator untuk contoh konfigurasi ini. non-statically-stableDesain adalah memodifikasi persentase panggilan lalu lintas AGA, mengedit grup titik akhir, atau menghapus titik akhir dari grup titik akhir selama gangguan. Pendekatan ini akan tergantung pada bidang kontrol AGA.

Amazon Shield Advanced

Bidang kontrol Amazon Shield Advanced terdiri dari semua API Lanjutan Shield publik, dan dihosting di us-east-1. Ini termasuk fungsionalitas seperti `CreateProtectionCreateProtectionGroup`,`AssociateHealthCheck`,,`DesribeDRTAccess`, dan`ListProtections`. Bidang data adalah perlindungan DDoS yang disediakan oleh Shield Advanced serta pembuatan metrik Shield Advanced. Shield Advanced juga menggunakan pemeriksaan kesehatan Route 53 (yang merupakan bagian dari bidang data Route 53), jika Anda telah mengonfigurasinya. Selama gangguan bidang kontrol, operasi tipe CRUDL untuk Shield Advanced mungkin tidak berfungsi, tetapi perlindungan DDoS yang dikonfigurasi untuk sumber daya Anda, serta respons terhadap perubahan pemeriksaan kesehatan, akan terus berfungsi.

Artinya, Anda tidak boleh mengandalkan bidang kontrol Shield Advanced di jalur pemulihan Anda. Meskipun bidang kontrol Shield Advanced tidak menyediakan fungsionalitas langsung yang biasanya Anda gunakan dalam situasi pemulihan, mungkin ada saat-saat ketika Anda melakukannya. Misalnya, desain stabil-statis akan memiliki sumber daya DR Anda sudah dikonfigurasi untuk menjadi bagian dari kelompok perlindungan dan memiliki pemeriksaan kesehatan yang terkait dengan mereka sebagai lawan mengkonfigurasi perlindungan itu setelah kegagalan terjadi. Ini mencegah tergantung pada bidang kontrol Shield Advanced untuk pemulihan.

Lampiran C - Layanan Single-Region

Berikut ini adalah daftar layanan, atau fitur spesifik dalam layanan tersebut (yang tercantum dalam tanda kurung setelah nama layanan), yang hanya tersedia di satu Wilayah. Panduan yang sama untuk menerapkan stabilitas statis yang disediakan untuk layanan global lainnya berlaku untuk layanan ini ketika Anda perlu merencanakan dependensi pada bidang kontrol dan bidang data mereka.

- Alexa for Business
- AWS Marketplace(AWS Marketplace KatalogAPI, Analisis AWS Marketplace Perdagangan, Layanan AWS Marketplace Hak)
- Billing and Cost Management AWS Cost Explorer(AWS , Laporan Biaya dan Penggunaan, Anggaran AWS , Savings Plans)
- AWS BugBust
- Amazon Mekanikal Turk
- Amazon Chime
- Amazon Chime SDK (PSTNaudio, pesan, identitas)
- AWS Chatbot
- AWS DeepRacer
- AWS Device Farm
- Amazon GameSparks

Kontributor

Kontributor untuk dokumen ini meliputi:

- Michael Haken, Arsitek Solusi Utama, Amazon Web Services

Revisi dokumen

Untuk pemberitahuan tentang pembaruan laporan ini, berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Revisi kecil	Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi lebih lanjut, lihat Praktik terbaik keamanan di IAM.	9 Nopember 2023
Publikasi awal	Whitepaper diterbitkan.	16 Nopember 2022

Glosarium AWS

Lihat terminologi AWS terbaru di AWS glosarium dalam Referensi Glosarium AWS.

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri terhadap informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik AWS produk saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak menciptakan komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok atau pemberi lisensinya. AWSproduk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, pernyataan, atau kondisi apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh AWS perjanjian, dan dokumen ini bukan bagian dari, juga tidak memodifikasi, perjanjian apa pun antara AWS dan pelanggannya.

© 2022 Amazon Web Services, Inc. atau afiliasinya. Semua hak dilindungi.

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