Panduan Pengguna

AWS Pengelolaan Akun

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

AWS Pengelolaan Akun: Panduan Pengguna

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 merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Akun AWS? 1
Fitur dari Akun AWS 3
Apakah Anda yang pertama kali AWS pengguna? 3
Support dan umpan balik 4
Lainnya AWS sumber daya 4
Bandingkan opsi pendaftaran 6
Didukung Layanan AWS untuk Mendaftar untuk AWS (baru) 6
Layanan AWS termasuk dalam Tingkat Gratis baru kami AWS pengalaman 7
Layanan AWS termasuk dalam Paket Berbayar baru kami AWS pengalaman 12
Layanan AWS tidak didukung untuk yang baru AWS pengalaman 13
Pertimbangan untuk memilih cara mendaftar AWS 18
Bandingkan fitur untuk opsi pendaftaran 19
Bandingkan manajemen akses 20
Kelola Akun AWS 22
Daftar untuk AWS (baru) 26
Mendaftar menggunakan Daftar untuk AWS (baru) 28
Langkah selanjutnya 29
Gunakan Peng AWS aturan 29
Hubungkan alat pengkodean AI 31
Pertimbangan untuk menghubungkan alat pengkodean Anda ke proyek Anda 31
Hubungkan alat pengkodean AI Anda ke proyek Anda 32
Bekerja dengan beberapa proyek 33
AWS tindakan untuk pemilik proyek 35
Perbarui kata sandi Anda 36
Kelola otentikasi multi-faktor (MFA) 37
Poin kunci 37
Jenis MFA yang tersedia untuk baru kami AWS pengalaman 38
Daftarkan perangkat MFA Anda 40
Daftarkan kunci keamanan sebagai perangkat MFA Anda 42
Ganti nama perangkat MFA Anda 42
Hapus perangkat MFA Anda 43
Hapus semua sesi 43
Kelola nama atau nama panggilan Anda 44
Ubah alamat email Anda 45

Mengedit informasi kontak Anda 45
Memilih tidak menggunakan konten Anda untuk peningkatan layanan 46
Minta data AWS Builder ID Anda 47
Membuat proyek 48
Pertimbangan untuk membuat proyek 48
Untuk membuat proyek 49
Wilayah AWS untuk proyek Anda 50
Temukan yang dipilih Wilayah AWS untuk proyek Anda 51
Negara-negara di mana sumber daya Regional disediakan di AS Timur (Ohio) (us-east-2) 51
Negara-negara tempat sumber daya Regional disediakan di Asia Pasifik (Sydney) (ap-southeast-2) 54
Negara-negara di mana sumber daya regional disediakan di Eropa (Stockholm) (eu-utara-1) 57
Kebijakan terkelola untuk organisasi Anda 64
Kebijakan kontrol layanan untuk proyek 64
Kebijakan kontrol layanan untuk Tingkat Gratis untuk proyek 86
Kebijakan kontrol layanan untuk Paket Berbayar untuk proyek 97
Kebijakan pengendalian sumber daya untuk proyek 109
Beralih antar proyek 111
Beralih antar proyek untuk sesi aktif dari Konsol Manajemen AWS 111
Beralih antar proyek di AWS Pengaturan 111
Beralih antar proyek dari Konsol Manajemen AWS 112
Undang anggota tim 112
Pertimbangan untuk anggota tim 113
Bagaimana anggota tim mengakses AWS sumber daya 114
Undang anggota tim 114
Mengundang anggota tim ke sebuah proyek 115
Menghapus anggota tim dari proyek 116
Menghapus anggota tim 116
Mencabut undangan 117
Mengirim ulang undangan 117
Tingkatkan akun Anda 118
Pertimbangan untuk meningkatkan akun Anda 118
Tingkatkan akun Anda 119
Buat batas pengeluaran 120

Apa itu batas pengeluaran? 120
Tetapkan batas pengeluaran Anda 120
Notifikasi 121
Sesuaikan pengaturan batas pengeluaran Anda dengan kontrol biaya awal opsional 121
Apa yang terjadi jika Anda mencapai batas Anda 123
Hal penting lainnya yang perlu diperhatikan 123
Buat batas pengeluaran di AWS Pengaturan 123
Memperbarui batas pengeluaran 124
Perbarui batas pengeluaran di AWS Pengaturan 124
Menghapus batas pengeluaran 125
Hapus batas pengeluaran di AWS Pengaturan 125
Tingkat Gratis 125
Melacak penggunaan Tingkat Gratis Anda 126
Dapatkan kredit tambahan 128
Lihat informasi penagihan Anda di AWS Pengaturan 128
Untuk melihat biaya berdasarkan proyek 129
Lihat riwayat penagihan Anda di AWS Pengaturan 129
Kelola metode pembayaran Anda 130
Lakukan pembayaran di AWS Pengaturan 131
Ubah mata uang pilihan Anda di AWS Pengaturan 131
Kelola pendaftaran pajak di AWS Pengaturan 132
Memperbarui dan menghapus nomor pendaftaran pajak 132
Mengelola pembebasan pajak AS Anda 133
Lihat dan tukarkan kredit 134
Kelola akun di India 135
Daftar untuk AWS (baru) dengan AWS India 135
Mengelola informasi verifikasi pelanggan 137
Menyiapkan penagihan Indonesia 141
Menambahkan atau mengedit Nomor Rekening Permanen 141
Mengedit beberapa Nomor Rekening Permanen 142
Mengedit beberapa nomor Pajak Barang dan Jasa 142
Melihat faktur pajak 142
Mengubah penjual catatan ke atau dari AWS India 143
Access AWS Support 145
Dukungan proyek 145
Dukungan teknis 146

Support jika semua proyek dan organisasi Anda ditutup 146
Mulai uji coba Dukungan Bisnis+ 146
Pantau proyek Anda 147
Pantau proyek Anda menggunakan AWS CloudTrail 148
Gunakan CloudTrail untuk melihat siapa yang memodifikasi proyek Anda 148
Menutup proyek 151
Apa yang perlu Anda ketahui sebelum menutup proyek Anda 151
Untuk menutup proyek 152
Post-closure periode 152
Membuka kembali proyek Anda 153
Aktifkan fitur-fitur canggih 153
Apa yang terjadi ketika Anda mengaktifkan fitur-fitur canggih 153
Akun proyek setelah Anda mengaktifkan fitur lanjutan 156
Bagaimana akan AWS Pengaturan berubah setelah saya mengaktifkan fitur lanjutan? 157
Bisakah saya masih membuat proyek di AWS Pengaturan setelah saya mengaktifkan fitur-fitur canggih? 158
Cara mempersiapkan untuk mengaktifkan fitur-fitur canggih 158
Cara mengaktifkan fitur-fitur canggih 159
Setelah Anda mengaktifkan fitur-fitur canggih 160
Tetapkan kata sandi pengguna root 160
Kelola anggota tenaga kerja 161
Ubah sumber identitas 163
Hapus kebijakan organisasi 164
Tutup akun Anda di Peng AWS aturan 166
Apa yang perlu Anda ketahui sebelum menutup akun manajemen Anda 166
Menutup proyek 167
Tutup akun manajemen Anda 167
Hapus Anda AWS ID Pembangun 167
Mendaftar untuk AWS (lanjutan) 169
Langkah 1: Buat akun Anda 170
Langkah 2: (Disarankan) Instal AWS CLI 172
Langkah 3: (Disarankan) Siapkan AWS MCP Server 173
Terkait AWS layanan 173
Menggunakan pengguna root 174
Mengakses akun Anda 175
Rencanakan struktur tata kelola Anda 176

Manfaat menggunakan banyak Akun AWS 177
Kapan harus digunakan AWS Organizations 179
Kapan harus digunakan AWS Control Tower 185
Memahami mode operasi API 185
Konfigurasikan akun Anda 189
Membuat atau memperbarui alias akun Anda 190
Aktifkan atau menonaktifkan Wilayah AWS di akun Anda 190
Perbarui tagihan untuk Anda Akun AWS 202
Perbarui email pengguna root email 202
Perbarui kata sandi pengguna root 207
Perbarui Anda Akun AWS name 208
Perbarui kontak alternatif untuk Anda Akun AWS 212
Perbarui kontak utama untuk Anda Akun AWS 221
Melihat pengidentifikasi akun Anda 232
Memecahkan masalah akun Anda 238
Masalah pembuatan akun 238
Masalah penutupan akun 239
Masalah lainnya 241
Kelola akun di India 242
Buat sebuah Akun AWS dengan AWS India 243
Kelola informasi verifikasi pelanggan Anda 245
Tutup akun Anda 251
Apa yang perlu Anda ketahui sebelum menutup akun Anda 251
Cara menutup akun Anda 253
Apa yang diharapkan setelah Anda menutup akun 256
Buka kembali akun Anda 257
Apa yang perlu Anda ketahui sebelum membuka kembali akun Anda 258
Cara membuka kembali akun Anda 258
Apa yang diharapkan setelah Anda membuka kembali akun Anda 259
Siapkan akun Anda untuk digunakan setelah dibuka kembali 259
Ketersediaan wilayah 259
Amankan akun Anda 260
Perlindungan data 261
AWS PrivateLink 262
Membuat Titik Akhir 262
Kebijakan Amazon VPC Endpoint 263

Kebijakan titik akhir 263
Identity and Access Management 264
Audiens 265
Mengautentikasi dengan identitas 265
Mengelola akses menggunakan kebijakan 266
AWS Manajemen Akun dan IAM 268
Identity-based contoh kebijakan 276
Menggunakan kebijakan berbasis identitas 280
Pemecahan masalah 283
AWS kebijakan yang dikelola 285
AWSAccountManagementReadOnlyAccess 286
AWSAccountManagementFullAccess 287
Pembaruan kebijakan 288
Validasi kepatuhan 288
Ketahanan 289
Keamanan infrastruktur 290
Pantau akun Anda 291
CloudTrail log 291
Informasi Manajemen Akun di CloudTrail 292
Memahami entri log Manajemen Akun 293
Memantau acara Manajemen Akun dengan EventBridge 296
Acara Manajemen Akun 297
Kuota 299
Riwayat dokumen 302
..... cccv

Apa itu Akun AWS?

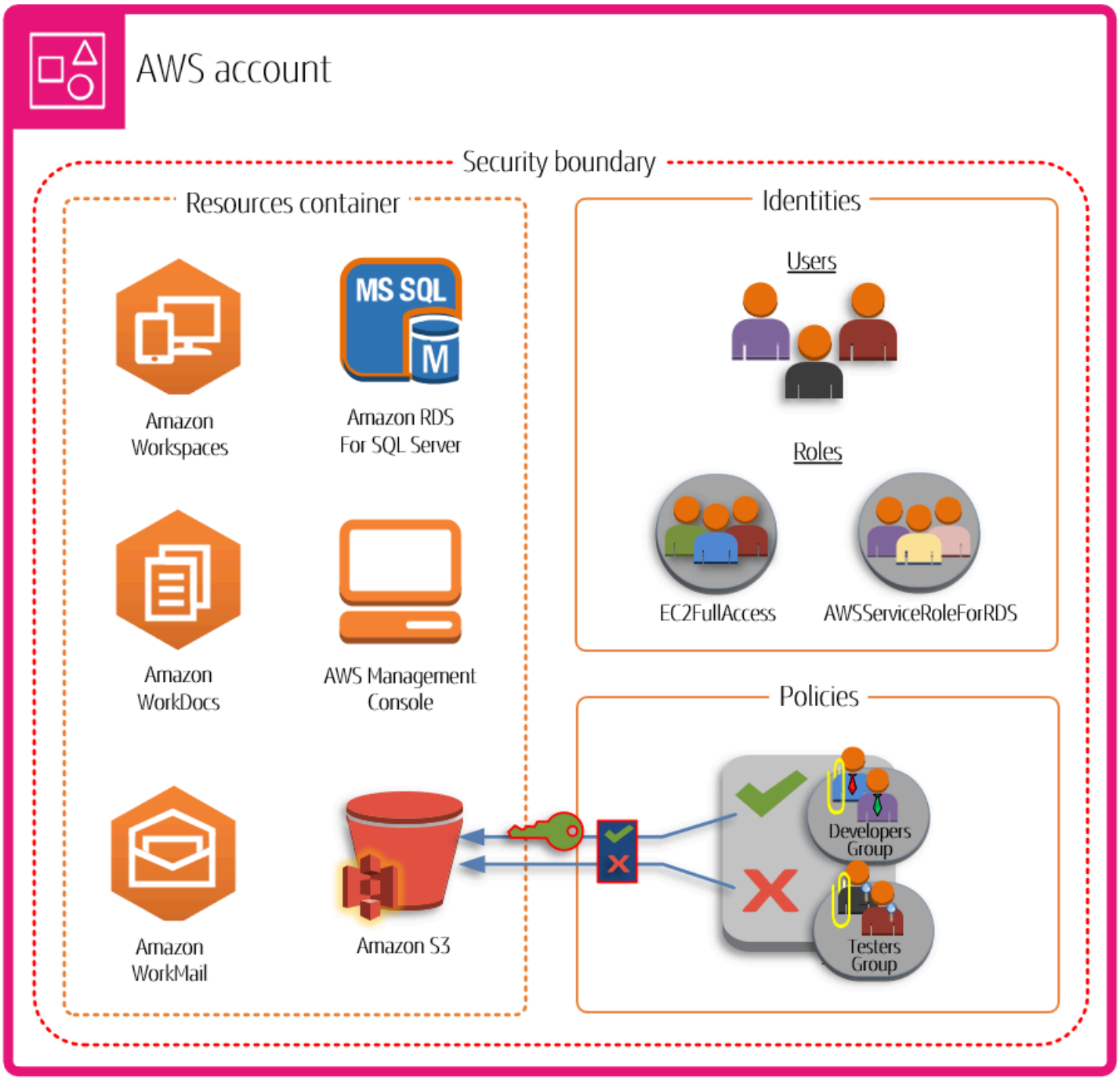
An Akun AWS mewakili hubungan bisnis formal yang Anda jalin dengan AWS. Anda membuat dan mengelola AWS sumber daya dalam Akun AWS, dan akun Anda menyediakan kemampuan manajemen identitas untuk akses dan penagihan. Masing-masing Akun AWS memiliki ID unik yang membedakannya dari yang lain Akun AWS.

Saat mendaftar AWS, Anda dapat memilih antara Mendaftar untuk AWS (baru) dan Daftar untuk AWS (lanjutan). Tergantung pada pilihan Anda, Anda memiliki akses ke Akun AWS atau proyek. Proyek berisi Akun AWS dan pengaturan untuk berbagi dengan kolaborator lain. Untuk informasi selengkapnya, lihat Bandingkan opsi pendaftaran.

Sumber daya dan data cloud Anda terkandung dalam Akun AWS. Akun bertindak sebagai batas isolasi manajemen identitas dan akses. Ketika Anda perlu berbagi sumber daya dan data antara dua akun, Anda harus secara eksplisit mengizinkan akses ini. Secara default, tidak ada akses yang diizinkan antar akun. Misalnya, jika Anda menetapkan akun yang berbeda untuk memuat sumber daya dan data produksi dan non-produksi, tidak ada akses yang diizinkan antara lingkungan tersebut secara default.

Akun AWS juga merupakan bagian mendasar dari mengakses AWS layanan. Seperti yang ditunjukkan pada ilustrasi berikut, an Akun AWS melayani dua fungsi utama:

- Wadah sumber daya — An Akun AWS adalah wadah dasar untuk semua AWS sumber daya yang Anda buat sebagai AWS pelanggan. Misalnya, bucket Amazon Simple Storage Service (Amazon S3), database Amazon Relational Database Service (Amazon RDS), dan instance Amazon Elastic Compute Cloud (Amazon EC2) adalah semua sumber daya. Setiap sumber daya diidentifikasi secara unik oleh Nama Sumber Daya Amazon (ARN) yang menyertakan ID akun akun yang berisi, atau memiliki, sumber daya.
- Batas keamanan — Akun AWS An juga merupakan batas keamanan dasar untuk AWS sumber daya Anda. Sumber daya yang Anda buat di akun tersedia untuk pengguna yang memiliki kredenSIAL untuk akun Anda. Di antara sumber daya utama yang dapat Anda buat di akun Anda adalah identitas, seperti pengguna dan peran. Identitas memiliki kredenSIAL yang dapat digunakan seseorang untuk masuk (mengo tentikasi). AWS Identitas juga memiliki kebijakan izin yang menentukan apa yang dapat dilakukan pengguna (otorisasi) dengan sumber daya di akun.



Menggunakan multi Akun AWS pel adalah praktik terbaik untuk menskalakan lingkungan Anda, karena memberikan batas penagihan alami untuk biaya, mengisolasi sumber daya untuk keamanan, memberikan fleksibilitas bagi individu dan tim, selain dapat beradaptasi untuk proses bisnis baru. Untuk informasi selengkapnya, lihat Manfaat menggunakan banyak Akun AWS.

Fitur dari Akun AWS

Akun AWS termasuk fitur inti berikut:

- Memantau dan mengontrol biaya — Akun adalah sarana default yang digunakan untuk AWS mengalokasikan biaya. Karena fakta ini, menggunakan akun yang berbeda untuk unit bisnis dan kelompok beban kerja yang berbeda dapat membantu Anda melacak, mengontrol, memprediksi, menganggarkan, dan melaporkan pengeluaran cloud Anda dengan lebih mudah. Selain pelaporan biaya di tingkat akun, AWS juga memiliki dukungan bawaan untuk mengkonsolidasikan dan melaporkan biaya di seluruh rangkaian akun Anda jika Anda memilih untuk digunakan AWS Organizations di beberapa titik. Anda juga dapat menggunakan Kuota AWS Layanan untuk membantu melindungi Anda dari penyediaan AWS sumber daya yang berlebihan dan tindakan berbahaya yang secara dramatis dapat berdampak pada AWS biaya Anda.
- Unit isolasi — An Akun AWS menyediakan batas keamanan, akses, dan penagihan untuk AWS sumber daya Anda yang dapat membantu Anda mencapai otonomi dan isolasi sumber daya. Secara desain, semua sumber daya yang disediakan dalam akun secara logis diisolasi dari sumber daya yang disediakan di akun lain, bahkan dalam lingkungan Anda sendiri AWS . Batas isolasi ini memberi Anda cara untuk membatasi risiko masalah terkait aplikasi, kesalahan konfigurasi, atau tindakan berbahaya. Jika masalah terjadi dalam satu akun, dampak terhadap beban kerja yang terdapat di akun lain dapat dikurangi atau dihilangkan.
- Mencerminkan beban kerja bisnis Anda — Gunakan beberapa akun untuk mengelompokkan beban kerja dengan tujuan bisnis yang sama di akun yang berbeda. Hasilnya, Anda dapat menyelaraskan kepemilikan dan pengambilan keputusan dengan akun tersebut dan menghindari dependensi dan konflik dengan cara beban kerja di akun lain diamankan dan dikelola. Bergantung pada model bisnis Anda secara keseluruhan, Anda dapat memilih untuk mengisolasi unit bisnis atau anak perusahaan yang berbeda di akun yang berbeda. Pendekatan ini juga dapat memudahkan divestasi unit-unit tersebut dari waktu ke waktu.

Apakah Anda yang pertama kali AWS pengguna?

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Jika Anda pengguna pertama kali AWS, langkah pertama Anda adalah mendaftar AWS. Anda dapat membuat Akun AWS tempat Anda memiliki kontrol penuh atas konfigurasi akun dan tempat penyimpanan konten Anda, yang diperlukan untuk beban kerja yang diatur seperti HIPAA atau FedRAMP, atau Anda dapat membuat Akun AWS dengan default yang telah dikonfigurasi sebelumnya. Untuk mengetahui pendaftaran mana yang tepat untuk Anda, lihatBandingkan opsi pendaftaran.

Untuk petunjuk langkah demi langkah tentang cara mengatur akun baru di mana Anda memiliki kontrol penuh atas pengaturan awal, lihatDaftar untuk AWS (lanjutan).

Untuk petunjuk langkah demi langkah tentang cara mengatur akun baru di mana membuat akun dengan AWS default yang telah dikonfigurasi sebelumnya, lihat. Daftar untuk AWS (baru)

Support untuk AWS Pengelolaan Akun

Anda dapat memposting umpan balik dan pertanyaan menggunakan forum dukungan Manajemen AWS Akun. Untuk informasi umum tentang AWS forum, lihat AWS re:Post.

Jika Anda tidak dapat menemukan jawaban yang Anda cari AWS re:Post, Anda dapat membuat akun atau kasus dukungan terkait penagihan menggunakan. Konsol Manajemen AWS Untuk informasi selengkapnya, lihat Contoh: Membuat kasus dukungan untuk akun dan penagihan.

Lainnya AWS sumber daya

- AWS Pelatihan dan Kursus - Tautan ke kursus berbasis peran dan khusus serta laboratorium mandiri untuk membantu mempertajam AWS keterampilan Anda dan mendapatkan pengalaman praktis.
- AWS Alat Pengembang — Tautan ke alat dan sumber daya pengembang yang menyediakan dokumentasi, contoh kode, catatan rilis, dan informasi lainnya untuk membantu Anda membangun aplikasi inovatif AWS.
- AWS Dukungan Center — Hub untuk membuat dan mengelola kasus AWS Support Anda. Juga mencakup tautan ke sumber daya yang bermanfaat lainnya, seperti forum, Pertanyaan Umum teknis, status kesehatan layanan, dan AWS Trusted Advisor.
- AWS Support — Halaman web utama untuk informasi tentang AWS Support, saluran dukungan respons cepat satu-satu untuk membantu Anda membangun dan menjalankan aplikasi di cloud.
- Hubungi Kami — Titik kontak pusat untuk pertanyaan tentang AWS penagihan, akun, acara, penyalahgunaan, dan masalah lainnya.

- AWS Ketentuan Situs — Informasi terperinci tentang hak cipta dan merek dagang kami; akun, lisensi, dan akses situs Anda; dan topik lainnya.

Bandingkan opsi pendaftaran

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Saat Anda mendaftar AWS, Anda membuka kunci cloud paling komprehensif dan diadopsi secara luas di dunia. Kami menawarkan pilihan terbaik dari kemampuan dan keahlian cloud dan AI yang inovatif, pada infrastruktur global yang paling luas, dengan keamanan, keandalan, dan kinerja terdepan di industri.

Ada dua cara untuk mendaftar AWS. Jika Anda ingin kontrol penuh atas konfigurasi akun dan di mana konten Anda disimpan, atau jika Anda memiliki beban kerja yang diatur seperti HIPAA, FedRAMP, gunakan. Daftar untuk AWS (lanjutan) Jika Anda adalah pengguna baru dan ingin menggunakan login yang sudah Anda miliki untuk masuk AWS dan membuat AWS lingkungan dengan default yang telah dikonfigurasi sebelumnya di pilih, gunakan. Wilayah AWSDaftar untuk AWS (baru)

Didukung Layanan AWS untuk Mendaftar untuk AWS (baru)

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Saat Anda menggunakan Daftar untuk AWS (baru), Anda mendapatkan akses ke Tingkat Gratis. Tingkat Gratis menyediakan akses ke AWS layanan tertentu. Anda dapat meningkatkan akun Anda ke Paket Berbayar untuk mengakses AWS layanan dan fitur tambahan. Untuk mempelajari cara meningkatkan akun Anda, lihatTingkatkan akun Anda di AWS Pengaturan.

Tidak semua AWS layanan tersedia untuk Daftar AWS (baru). Jika layanan tidak tercantum dalam salah satu daftar berikut atau memiliki fitur yang tidak didukung, Anda harus membuat akun dengan menggunakan Daftar untuk AWS (lanjutan) atauAktifkan lanjutan AWS fitur.

Layanan AWS termasuk dalam Tingkat Gratis baru kami AWS pengalaman

AWS Layanan berikut termasuk dalam Tingkat Gratis Mendaftar untuk AWS (baru). Multi-Region atau Fitur lintas wilayah tidak didukung untuk layanan apa pun. Untuk informasi selengkapnya, lihat Wilayah AWS untuk proyek Anda.

- Amazon API Gateway
- Amazon Athena
- Amazon AppFlow
- AWS App2Container
- Amazon Augmented AI
- Amazon Bedrock
- Inti Agen Batuan Dasar Amazon
- Amazon CloudFront
  - Lambda @Edge tidak didukung.
- Amazon CloudWatch
- CloudWatch Log Amazon
- Amazon CodeGuru Profiler
- Amazon Cognito
- Amazon Cognito Sync
- Amazon DynamoDB
- Amazon DataZone
- Registri Wadah Elastis Amazon (ECR)
- EC2 Image Builder
- Amazon EKS Anywhere
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
  - Blok Kapasitas Pembelian dan Ekstensi Blok Kapasitas Pembelian tidak didukung.
- Amazon Elastic Container Registry Publik
- Amazon Elastic Container Service

- LAYANAN AMAZON ELASTIC KUBERNETES
- Sistem File Elastis Amazon
- Amazon ElastiCache
- Amazon EventBridge
- Amazon Lex
- Amazon Lightsail
- Amazon Location Service
- Amazon Managed Service for Prometheus
- Amazon Managed Workflows for Apache Airflow
- Amazon MQ
- OpenSearch Layanan Amazon
- Amazon Polly
- Amazon Quick
  - Hanya Amazon Quick Free atau Quick Plus yang didukung. Untuk informasi selengkapnya, lihat Harga Cepat Amazon.
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon Route 53
- Amazon SageMaker
- Amazon SageMaker AI
- Studio SageMaker Terpadu Amazon
- Layanan Email Sederhana Amazon
- Layanan Notifikasi Sederhana Amazon
- Amazon Simple Queue Service
- Amazon Simple Storage Service
  - Hibah Akses Amazon S3 tidak didukung.
- Layanan Alur Kerja Sederhana Amazon
- Izin Terverifikasi Amazon
- Cloud Privat Virtual Amazon

- Amazon Aurora
- Amazon Aurora DSQL
- AWS Amplify
- AWS AppConfig
- AWS AppSync
- Penskalaan Otomatis Aplikasi
- AWS Transform MGN
- AWS Artifact
  - (HIPAA) AWS Business Associate Addendum, (HIPAA) AWS Organizations Business Associate Addendum, SEC Rule 17a-4 Addendum AWS , dan SEC Rule 18a-6 Adendum tidak didukung. AWS
- AWS B2B Pertukaran Data
- Agen AWS Backint
- AWS Backup
- AWS Batch
- AWS Manajemen Penagihan dan Biaya
  - Gunakan AWS Pengaturan untuk mengatur tagihan Anda, membuat batas pengeluaran untuk mengontrol biaya Anda, dan mengambil dan membayar faktur. Anda menggunakan Billing and Cost Management untuk membuat anggaran, menganalisis, dan mengoptimalkan biaya Anda. Untuk informasi selengkapnya, lihat Menggunakan konsol Billing and Cost Management dengan pengalaman AWS baru kami.
- AWS Budgets
- AWS Certificate Manager
  - AWS Sertifikat publik yang dapat diekspor oleh Certificate Manager tidak didukung.
- AWS Cloud Control API
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudShell
- AWS CloudTrail

- AWS CodeArtifact
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Compute Optimizer
- AWS Config
- AWS Console Mobile Application
- AWS Cost Explorer
- AWS Data Pipeline
- AWS Transfer Data
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- Media Sosial Olah Pesan Pengguna Akhir AWS
- Resolusi Entitas AWS
- AWS Glue
- AWS Health
- AWS Identity and Access Management
- AWS IoT
  - AWS Greengrass tidak didukung.
- AWS IoT Pembela Perangkat
- AWS IoT Manajemen Perangkat
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- AWS Lake Formation
- AWS Lambda
  - Lambda @Edge tidak didukung.
- AWS Launch Wizard

- AWS License Manager
- Konsol Manajemen AWS
- AWS Marketplace
  - Bedrock dan Gratis saja.
- AWS Network Manager
- AWS Payment Cryptography
- AWS PrivateLink
- AWS Resource Access Manager (RAM)
- Penjelajah Sumber Daya AWS
- AWS Resource Groups
- Route 53 Pengontrol Pemulihan Aplikasi Amazon (ARC)
- AWS SDK & Alat
- AWS Secrets Manager
- AWS Security Token Service
- AWS Serverless Application Repository
- Service Quotas
- AWS Signer
- AWS Step Functions
- AWS Dukungan
- AWS Systems Manager
- Manajer Sistem AWS untuk SAP
- Notifikasi Pengguna AWS
  - User-configured notifikasi dan operasi konfigurasi pemberitahuan terkelola tidak didukung. Untuk informasi selengkapnya, lihat Apa itu Pemberitahuan AWS Pengguna?
- AWS WAF
  - AWS Shield tidak didukung.
- AWS Well-Architected Tool
- AWS X-Ray
- AWS CodeBuild

- Elastic Load Balancing
- AWS SQL Workbench
- OpenSearch Layanan Amazon Tanpa Server
- Amazon Timestream

Untuk melihat kebijakan yang mengontrol akses ke layanan Tingkat Gratis, lihatKebijakan kontrol layanan untuk Tingkat Gratis untuk proyek.

Layanan AWS termasuk dalam Paket Berbayar baru kami AWS pengalaman

Layanan berikut tersedia untuk Mendaftar AWS (baru) jika Anda memiliki Paket Berbayar. Untuk informasi lebih lanjut, lihatTingkatkan akun Anda di AWS Pengaturan. Multi-Region atau Fitur lintas wilayah tidak didukung untuk layanan apa pun. Untuk informasi selengkapnya, lihat Wilayah AWS untuk proyek Anda.

- DevOpsGuru Amazon
- Amazon DocumentDB (dengan kompatibilitas MongoDB)
- Amazon EMR
- Amazon Forecast
- Amazon Glacier
- Amazon Kinesis
- Amazon Kinesis Data Streams
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- Amazon Managed Blockchain
- Amazon Managed Streaming untuk Apache Kafka
- Amazon MemoryDB
- Amazon Neptune
- Amazon Personalize
- Amazon Redshift
- S3 Glacier Deep Archive

- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS AppFabric
- AWS Data Exchange
- AWS Olah Pesan Pengguna Akhir SMS
- AWS Fault Injection Service
- AWS Firewall Manager
- AWS Network Firewall
- AWS Agen Keamanan
- AWS Storage Gateway
- DevOps Agen

Untuk melihat kebijakan yang mengontrol akses ke layanan Paket Berbayar, lihatKebijakan kontrol layanan untuk Paket Berbayar untuk proyek.

Layanan AWS tidak didukung untuk yang baru AWS pengalaman

AWS Layanan berikut tidak didukung untuk AWS pengalaman baru kami, kecuali AndaAktifkan lanjutan AWS fitur. AWS Layanan ini tidak diperlukan untuk pengembang baru atau tim kecil. Beberapa layanan ini secara otomatis diaktifkan untuk akun Anda dan dikelola oleh AWS. Untuk informasi selengkapnya, lihat Bandingkan fitur untuk opsi pendaftaran.

- Alexa for Business
- Alexa Top Sites
- Alexa Web Information Service
- Amazon Braket
- Amazon Chime
- Amazon Chime Business Memanggil layanan yang dijual oleh AMCS LLC
- Amazon Chime Hubungi Saya
- Amazon Chime Call Me layanan yang dijual oleh AMCS LLC
- Amazon Chime Dial Dalam layanan yang dijual oleh AMCS LLC

- Amazon Chime Dialin
- Fitur Amazon Chime
- Amazon Chime SDK
- Layanan Amazon Chime
- Amazon Chime SMS
- Amazon Chime Voice Connector layanan yang dijual oleh AMCS LLC
- Direktori Cloud Amazon
- Amazon CloudSearch
- Amazon CodeWhisperer
- Pelanggan Amazon Connect
- Profil Pelanggan Pelanggan Amazon Connect
- ID Suara Pelanggan Amazon Connect
- AWS Deadline Cloud
- Amazon Detective
- Amazon Elastic Inference
- Amazon Elastic Transcoder
- Amazon FinSpace
- Armada Fleksibel Amazon
- Amazon Fraud Detector
- Amazon FSx
- GameLift Peladen Amazon
- GameLift Aliran Amazon
- Amazon GameSparks
- Amazon GuardDuty
- AWS HealthOmics
- Amazon Inspector Klasik
- Amazon Interactive Video Service
- Obrolan Amazon IVS

- Amazon Kendra
- Amazon Keyspaces (untuk Apache Cassandra)
- Kiro
- Amazon Macie
- Amazon Managed Grafana
- Amazon Mechanical Turk
- Hadiah Pekerja Amazon Mechanical Turk
- Amazon Mobile Analytics
- Amazon Monitron
- Amazon Nimble Studio
- OpenSearch Layanan Konsumsi Layanan Amazon
- Amazon Q
- Amazon Q Bisnis
- Amazon Q Developer
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon S3 on Outposts
- Amazon SageMaker Ground Truth
- Amazon Security Lake
- Amazon Sumerian
- Amazon WorkDocs
- Amazon WorkSpaces
- WorkSpaces Contoh Amazon
- WorkSpaces Aplikasi Amazon (WorkSpaces Aplikasi Amazon)
- Klien WorkSpaces Tipis Amazon
- WorkSpaces Web Amazon
- Amazon WorkLink
- Amazon WorkMail
- AWS Profiler Biaya Aplikasi

- AWS Clean Rooms
- AWS Studio Aplikasi
- AWS Application Discovery Service
- AWS Audit Manager
- AWS Billing Conductor
- AWS CloudHSM
- AWS Client VPN
- AWS Awan WAN
- AWS Control Tower
- AWS Layanan Migrasi Database
- AWS DeepRacer
- AWS Device Farm
- AWS Direct Connect
- AWS Elastic Disaster Recovery
- AWS Elemental Live
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- AWS Global Accelerator
- AWS Ground Station
- AWS HealthImaging
- AWS IAM Identity Center
- AWS Identity and Access Management Access Analyzer
- AWS Interkoneksi
- AWS IoT Acara

- AWS IoT FleetWise
- AWS IoT RoboRunner
- AWS Mainframe Modernization
- AWS Migration Hub
- AWS Migration Hub Refactor Spaces
- AWS Modular Data Center
- AWS OpsWorks
- AWS Organizations
- AWS Outposts
- AWS Parallel Computing Service
- AWS Partner Network
- AWS Kalkulator Harga
- AWS Private Certificate Authority
- AWS Proton
- AWS re:Post Privat
- AWS Resilience Hub
- AWS RoboMaker
- AWS Kain RTB
- AWS Security Hub
- Respons Insiden Keamanan AWS
- AWS Service Catalog
- AWS Shield
- AWS SimSpace Weaver
- AWS Snowball
- Rantai Pasokan AWS
- Pembuat Jaringan Telekomunikasi AWS
- AWS Transform
- AWS Transfer Family
- AWS Transit Gateway

- AWS Trusted Advisor
- Akses Terverifikasi AWS
- Site-to-Site VPN
- Kisi VPC Amazon
- AWS Wickr
- Amazon CodeCatalyst
- Amazon Comprehend Medical
- Konferensi Telekomunikasi (layanan yang dijual oleh AMCS LLC)
- Contact Center Telekomunikasi (layanan yang dijual oleh AMCS LLC)
- Pusat Kontak Telekomunikasi Korea
- Pusat Kontak Telekomunikasi Afrika Selatan
- DynamoDB Accelerator
- Layanan VMware Amazon Elastic
- Oracle Database@AWS
- Layanan OpenShift Red Hat di AWS
- AWS App Runner

Pertimbangan untuk memilih cara mendaftar AWS

Pertimbangkan hal berikut sebelum memilih metode pendaftaran Anda. Anda dapat mengaktifkan semua AWS fitur untuk akun Anda jika perlu.

- Jika Anda memiliki persyaratan produk tertentu seperti beban kerja yang diatur yang mencakup HIPAA atau FedRAMP, jangan gunakan pengalaman baru kami. AWS
- Konten Anda akan disimpan di Wilayah yang ditunjuk yang dipilih berdasarkan informasi kontak Anda.
- AWS Pengalaman baru memudahkan Anda untuk mulai membangun tanpa membuat AWS izin. Jika Anda memerlukan kontrol halus atas pengguna atau izin berbasis peran, jangan gunakan Daftar untuk (baru). AWS
- Jika Anda memerlukan konfigurasi pembayaran khusus akun yang diatur oleh AWS, juga dikenal sebagai penagihan persyaratan bersih, jangan gunakan Daftar untuk AWS (baru).

- Jika Anda memerlukan akses ke set lengkap AWS layanan, jangan gunakan Daftar untuk AWS (baru). Untuk informasi selengkapnya, lihat Didukung Layanan AWS untuk Mendaftar untuk AWS (baru).

Bandingkan fitur untuk opsi pendaftaran

Tabel berikut membandingkan persyaratan AWS luas yang didukung untuk Mendaftar untuk AWS (baru) atau Mendaftar untuk AWS (lanjutan). Jika fitur tidak tercantum dalam tabel ini atau dijelaskan dalamBandingkan manajemen akses, itu tersedia. Anda dapat mengaktifkan fitur-fitur canggih untuk akun Anda jika Anda memerlukan salah satu fitur yang tidak didukung. Untuk informasi selengkapnya, lihat Aktifkan lanjutan AWS fitur.

Fitur	Mendaftar untuk AWS (baru)	Mendaftar untuk AWS (lanjutan)
Bergabunglah dengan Jaringan AWS Mitra	Tidak	Ya
Buat kontrak Layanan Profesional	Tidak	Ya
Mendaftar dalam Perjanjian Perusahaan dengan AWS	Tidak	Ya
Beli langganan AWS Skill Builder Team	Tidak	Ya
Bekerja dengan Mitra AWS Pelatihan	Tidak	Ya
Dapatkan kredit tambahan dari AWS Activate	Tidak	Ya
Gunakan AWS Marketplace	Tidak	Ya
Tentukan AWS akun Anda sebagai HIPAA atau SEC compliant	Tidak	Ya
Pilih yang spesifik Wilayah AWS untuk membuat sumber daya Regional Anda	Tidak. Untuk informasi lebih lanjut, lihatWilayah AWS untuk proyek Anda.	Ya
Mengakses Wilayah keikutsertaan	Tidak	Ya

Fitur	Mendaftar untuk AWS (baru)	Mendaftar untuk AWS (lanjutan)
Penganalisis Akses IAM	Tidak	Ya
Sign-in kebijakan akses	Tidak	Ya
Buat batas pengeluaran untuk akun Anda	Ya	Tidak
Paket tabungan	Tidak	Ya
Keikutsertaan otomatis ke Hub Pengoptimalan Biaya untuk Paket Berbayar	Ya	Tidak
Keikutsertaan otomatis ke AWS Organizations	Ya	Tidak
Keikutsertaan otomatis ke Pusat Identitas IAM	Ya	Tidak
Secara otomatis ikut serta ke manajer peran IAM	Ya	Tidak
Warna akun konsol	Tidak	Ya
Gunakan AWS Console Mobile Application	Tidak	Ya
Nonaktifkan dukungan konsol multi-sesi	Tidak	Ya. Jika Anda masuk lagi menggunakan Builder ID, dukungan multi-sesi akan diaktifkan secara otomatis.

Bandingkan manajemen akses

Saat Anda menggunakan AWS pengalaman baru kami, AWS buat default yang telah dikonfigurasi sebelumnya untuk membantu Anda mulai membangun. AWS Sumber daya Anda diatur dalam proyek. Sebuah proyek berisi Akun AWS, yang disebut akun proyek, dan pengaturan untuk berbagi dengan kolaborator lain. Jika Anda menggunakan paket berbayar, proyek Anda juga dapat memiliki biaya sebelum pajak bulanan yang ditetapkan, yang disebut batas pengeluaran. Semua proyek yang

Anda miliki membentuk organisasi Anda, yang Anda kontrol melalui akun manajemen Anda di AWS Pengaturan. Organisasi ini sama dengan AWS Organisasi; Namun, AWS mengelola aspek-aspek organisasi ini atas nama Anda.

AWS mengelola elemen-elemen berikut dari AWS Organisasi Anda:

- Kebijakan manajemen organisasi. Saat Anda menggunakan AWS pengalaman baru kami, AWS mengelola kebijakan manajemen organisasi termasuk kebijakan pengendalian sumber daya (RCP) dan kebijakan kontrol layanan (SCP). Jika Anda ingin membuat sendiri, gunakan Daftar untuk AWS (lanjutan).
- Peran akses manusia. Peran akses manusia adalah peran apa pun yang memberikan izin khusus manusia. AWS memberi Anda dan anggota tim Anda akses administrator ke proyek Anda. Sebagai pemilik proyek, Anda dapat menambah dan menghapus anggota tim. Untuk informasi selengkapnya, lihat Undang anggota tim untuk berkolaborasi AWS Pengaturan. Anda tidak membuat pengguna root. ID AWS Builder Anda memiliki akun project Anda, bukan alamat email pengguna root, dan ini tidak berubah saat Anda mengaktifkan fitur lanjutan. Anda dapat membuat peran IAM dan pengguna IAM jika perlu, tetapi mereka hanya dapat digunakan untuk akses terprogram, bukan akses konsol.

Setiap proyek memiliki implementasi keamanan terkelola yang membuatnya mudah dibangun dengan percaya diri. Secara default, aplikasi atau kode apa pun dalam proyek Anda memiliki akses ke semua AWS sumber daya dalam proyek yang sama. Anda tidak perlu melakukan konfigurasi akses tambahan.

AWS sumber daya dalam proyek yang berbeda tidak dapat saling mengakses, kecuali jika Anda mengaktifkan akses lintas proyek untuk sumber daya tertentu. Misalnya, Anda dapat membuat fungsi Lambda dalam satu proyek dan kemudian memanggilnya menggunakan API dalam proyek yang berbeda. Ini digambarkan sebagai integrasi lintas akun. Untuk informasi selengkapnya, lihat Integrasi Cross-accountLambda. Selama kedua proyek dimiliki oleh akun manajemen yang sama, ini didukung.

Secara default, proyek Anda tidak menyediakan akses eksternal ke sumber daya apa pun. Anda harus mengonfigurasi AWS sumber daya untuk memungkinkan akses publik. Anda dapat melakukan tindakan berikut:

- Buat bucket S3 publik untuk meng-host situs web atau file statis sederhana. Untuk informasi selengkapnya, lihat Memulai dengan Amazon S3.

- Buat API Gateway API untuk bertindak sebagai pintu depan aplikasi Anda. Untuk informasi selengkapnya, lihat Membangun API HTTP.
- Buat instans EC2 dengan alamat IP publik untuk memungkinkan komunikasi antara instans Anda dan internet. Untuk informasi selengkapnya, lihat Meluncurkan instans EC2 pertama Anda.
- Buat CloudFront distribusi untuk mengirimkan konten web statis dan dinamis Anda, seperti .html, .css, .js, dan file gambar, kepada pengguna Anda. Untuk informasi selengkapnya, lihat Memulai dengan CloudFront.
- Buat URL fungsi Lambda untuk menyediakan titik akhir HTTP sederhana dan langsung yang dapat diakses publik untuk fungsi Lambda. Pastikan fungsi Lambda Anda memiliki izin yang benar. Untuk informasi selengkapnya, lihat Membuat URL fungsi dan model Keamanan dan autentikasi untuk URL fungsi Lambda.
- Gunakan kombinasi AWS mekanisme ini atau lainnya.

Selain itu, ketika Anda mengaktifkan fitur-fitur canggih, Anda memiliki akses ke lebih banyak mekanisme untuk menyediakan akses eksternal ke sumber daya Anda.

Kelola Akun AWS

Anda mengelola Akun AWS berdasarkan jenis yang AWS Anda gunakan. Tabel berikut menunjukkan di mana menemukan dokumentasi untuk setiap tugas manajemen.

Tugas	Daftar untuk AWS (baru)	Daftar untuk AWS (lanjutan)
Mendaftar	Daftar untuk AWS (baru)	Daftar untuk AWS (lanjutan)
Buat akun	Buat proyek di AWS Pengaturan	Daftar untuk AWS (lanjutan)
Tutup akun	Menutup proyek di AWS Pengaturan	Tutup Akun AWS
Perbarui kata sandi Anda	Perbarui kata sandi Anda di AWS Pengaturan	Perbarui kata sandi pengguna root

Tugas	Daftar untuk AWS (baru)	Daftar untuk AWS (lanjutan)
Daftarkan perangkat MFA	Kelola otentikasi multi-faktor (MFA) di AWS Pengaturan	Langkah 3: (Disarankan) Siapkan AWS MCP Server
Ubah email Anda	Ubah alamat email Anda di AWS Pengaturan	Perbarui alamat email pengguna root
Ubah nama Anda	Kelola nama atau nama panggilan Anda di AWS Pengaturan	Perbarui Anda Akun AWS name
Perbarui informasi kontak	Mengedit informasi kontak Anda di AWS Pengaturan	Perbarui kontak utama untuk Anda Akun AWS
Perbarui kontak alternatif	Tidak berlaku	Perbarui kontak alternatif untuk Anda Akun AWS
Kelola penagihan	Kelola metode pembayaran Anda di AWS Pengaturan	Perbarui tagihan untuk Anda Akun AWS
Mengelola informasi pajak	Kelola pendaftaran pajak di AWS Pengaturan	Kelola pembayaran Anda
Aktifkan atau nonaktifkan Wilayah AWS	Tidak berlaku. Anda tidak dapat memodifikasi Wilayah AWS.	Aktifkan atau menonaktifkan Wilayah AWS di akun Anda
Lihat pengenal akun	Tidak berlaku	Tampilan Akun AWS pengidentifikasi

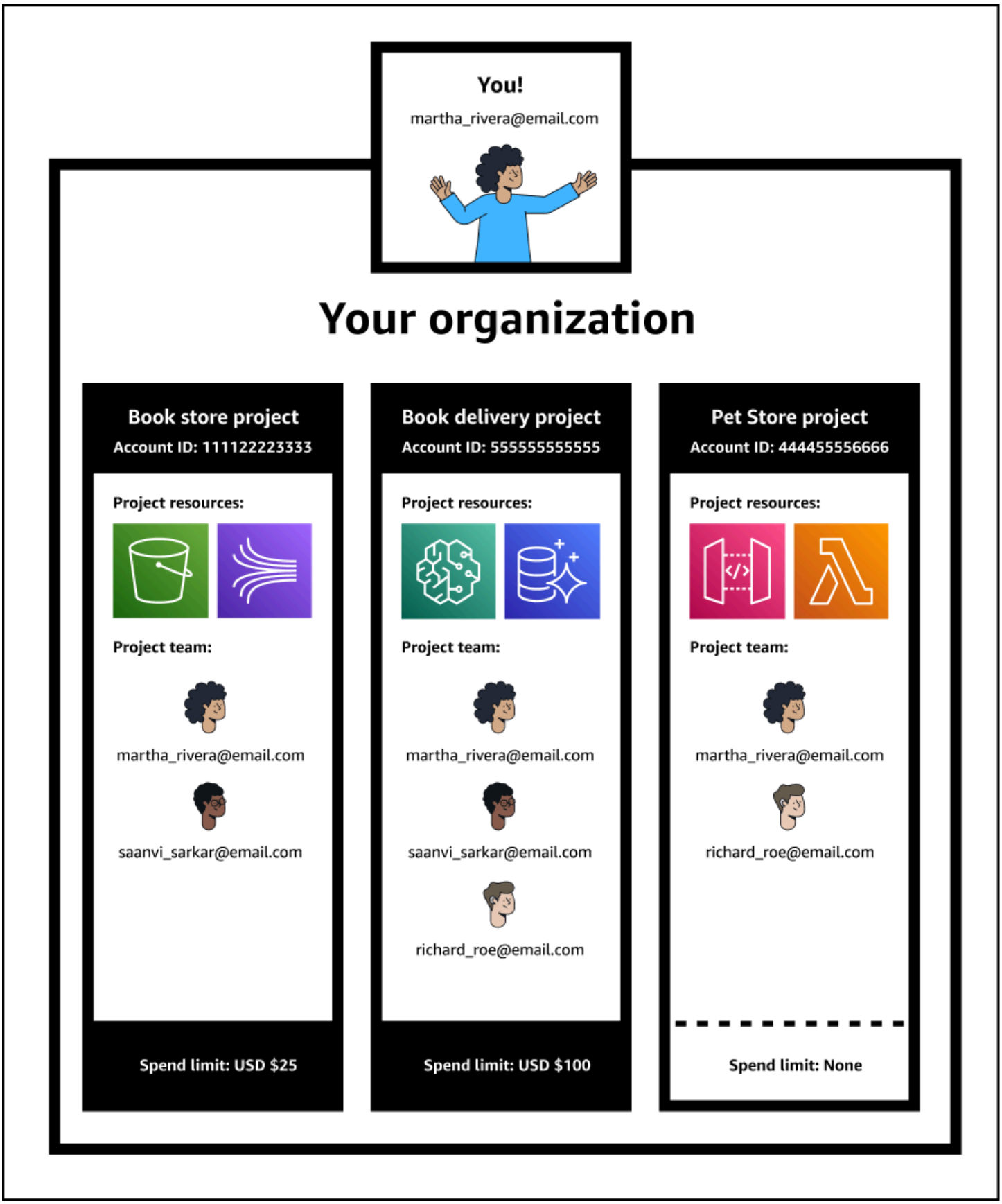
Tugas	Daftar untuk AWS (baru)	Daftar untuk AWS (lanjutan)
Buat alias akun	Tidak berlaku	Buat Akun AWS alias
Tingkatkan akun Anda	Tingkatkan akun Anda di AWS Pengaturan	Paket Tingkat Gratis
Buat batas pengeluaran	Buat batas pengeluaran di AWS Pengaturan	Tidak berlaku
Perbarui batas pengeluaran	Perbarui batas pengeluaran di AWS Pengaturan	Tidak berlaku
Hapus batas pengeluaran	Hapus batas pengeluaran di AWS Pengaturan	Tidak berlaku
Undang anggota tim	Undang anggota tim untuk berkolaborasi AWS Pengaturan	Identitas IAM
Beralih antar proyek	Beralih antar proyek	Multi-session dukungan
Connect alat pengkodean AI	Hubungkan alat pengkodean AI	Tidak berlaku
Hapus semua sesi	Hapus semua sesi di AWS Pengaturan	Tidak berlaku
Menyisih dari penggunaan data AI	Memilih tidak menggunakan konten Anda untuk peningkatan layanan di AWS Pengaturan	Kebijakan opt-out layanan AI

Tugas	Daftar untuk AWS (baru)	Daftar untuk AWS (lanjutan)
Minta data Anda	Minta Anda AWS Data ID Pembangun	Minta data Anda
Hapus AWS profil Anda	Tutup akun Anda di AWS Pengaturan	Tutup Akun AWS
Kelola akun di India	Kelola akun di India di AWS Pengaturan	Kelola akun di India
Buat pengguna administrator	Tidak berlaku	Daftar untuk AWS (lanjutan)
Rencanakan struktur tata kelola akun Anda	Tidak berlaku	Rencanakan Anda Akun AWS struktur tata kelola

Daftar untuk AWS (baru)

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Saat Anda menggunakan Daftar untuk AWS (baru), Anda membuat AWS lingkungan yang telah dikonfigurasi sebelumnya yang memungkinkan Anda menggunakan login yang sudah Anda miliki seperti Google atau GitHub untuk mengakses AWS sumber daya Anda. Sumber daya Anda diatur dalam proyek. Sebuah proyek berisi Akun AWS dan pengaturan untuk berbagi dengan kolaborator lain. Jika Anda menggunakan paket berbayar, proyek Anda juga dapat memiliki biaya sebelum pajak bulanan yang ditetapkan, yang disebut batas pengeluaran. Semua proyek yang Anda miliki membentuk organisasi Anda. Anda mengelola organisasi, mengakses proyek, dan menambahkan anggota tim di AWS Pengaturan.


You!
martha_rivera@email.com
Your organization
Book store project
Account ID: 111122223333
Project resources:
Project team:
martha_rivera@email.com
saanvi_sarkar@email.com
Spend limit: USD $25
Book delivery project
Account ID: 555555555555
Project resources:
Project team:
martha_rivera@email.com
saanvi_sarkar@email.com
richard_roe@email.com
Spend limit: USD $100
Pet Store project
Account ID: 444455556666
Project resources:
Project team:
martha_rivera@email.com
richard_roe@email.com
Spend limit: None

Saat Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (baru), buat AWS juga ID AWS Builder akun, yang merupakan profil pribadi yang mewakili Anda sebagai individu. Anda hanya dapat memiliki satu ID AWS Builder untuk setiap alamat email. Jika Anda telah membuat ID AWS Builder tetapi belum membuat Akun AWS, Anda mungkin memiliki beberapa pengaturan yang sudah dibuat untuk Anda dan Anda harus memodifikasinya nanti.

Untuk informasi selengkapnya tentang Mendaftar untuk AWS (baru), lihat dokumentasi berikut:

- Bandingkan opsi pendaftaran
- Didukung Layanan AWS untuk Mendaftar untuk AWS (baru)

Mendaftar menggunakan Daftar untuk AWS (baru)

Saat Anda mendaftar AWS, kami mungkin meminta informasi pembayaran. Proses verifikasi kami menahan USD $1 (atau setara) selama 3-5 hari untuk memverifikasi akun Anda dan mencegah penipuan. Anda tidak akan dikenakan biaya sampai Anda meningkatkan ke paket berbayar. Anda dapat mengelola metode pembayaran atau menutup akun kapan saja melalui AWS Pengaturan. Selain itu, ketika Anda mendaftar AWS, Anda mungkin tidak memenuhi syarat untuk Tingkat Gratis. Dalam hal ini, Anda harus memberikan informasi pembayaran Anda, dan Anda akan ditempatkan pada Paket Berbayar. Saat Anda menggunakan Paket Berbayar, Anda dapat menetapkan batas pengeluaran untuk beroperasi dalam anggaran yang dapat diprediksi dan terkendali.

Mendaftar untuk dukungan AWS (baru) menggunakan Google, GitHub, Apple, atau Amazon untuk akun Anda. Jika Anda sudah masuk ke akun Google di browser Anda, akun itu akan digunakan saat Anda mendaftar AWS.

Untuk mendaftar AWS menggunakan Daftar untuk AWS (baru)

1. Buka AWS halaman Daftar untuk.
2. Masukkan email Anda atau pilih login seperti Google, Apple GitHub, atau Amazon.
3. Jika Anda menggunakan login yang sudah Anda miliki, Anda akan diarahkan ke login untuk penyedia Anda. Setelah masuk, Anda akan diarahkan untuk AWS mendaftar.
4. Masukkan nama Anda dan pilih Lanjutkan.

   Nama ini dibagikan dengan anggota tim saat Anda memberi mereka akses ke proyek Anda.
5. Verifikasi email yang terkait dengan login Anda dengan memasukkan kode verifikasi. Setelah memverifikasi email, pilih Lanjutkan.

Email ini dibagikan dengan anggota tim saat Anda memberi mereka akses ke proyek Anda.

6. Masukkan kata sandi yang kuat untuk akun Anda dan pilih Lanjutkan.

   AWS mengharuskan kata sandi Anda memenuhi ketentuan berikut:

   - Itu harus memiliki minimal 8 karakter dan maksimal 128 karakter.
   - Ini harus mencakup minimal tiga dari campuran tipe karakter berikut: huruf besar, huruf kecil, angka, dan! @ # $% ^ & * () <> [] {} | _+-= simbol.
   - Itu tidak boleh identik dengan Akun AWS nama atau alamat email Anda.

7. Masukkan detail kontak Anda dan pilih Lanjutkan.
8. AWS akan menyediakan proyek pertama Anda di salah satu dari tiga Wilayah AWS dengan nama baru. Untuk informasi selengkapnya, lihat Wilayah AWS untuk proyek Anda. Anda dapat mengubah nama kapan saja.

Anda sekarang dapat mengakses Konsol Manajemen AWS. Untuk mengakses AWS Pengaturan, pilih Kelola proyek dari Konsol Manajemen AWS. Di AWS Pengaturan, Anda dapat mengundang anggota tim, membuat proyek baru, dan memodifikasi penagihan dan pengaturan lainnya.

Langkah selanjutnya

Setelah mendaftar AWS, Anda dapat menghubungkan alat pengkodean AI, menambahkan anggota tim untuk berkolaborasi, dan jika Anda memiliki paket berbayar, buat batas pengeluaran.

- Hubungkan alat pengkodean AI
- Undang anggota tim untuk berkolaborasi AWS Pengaturan
- Buat batas pengeluaran di AWS Pengaturan

Gunakan AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

AWS Peng aturan adalah tempat Anda mengelola dan mengakses proyek Anda. AWS Pengaturan tersedia saat Anda mendaftar menggunakan Daftar untuk AWS (baru). Anda dapat menggunakan AWS Pengaturan untuk melakukan hal berikut:

- Buat dan akses proyek yang Anda miliki. Untuk informasi selengkapnya, lihat Buat proyek di AWS Pengaturan.
- Akses proyek yang telah dibagikan dengan Anda.
- Undang anggota tim untuk berkolaborasi dalam proyek Anda. Untuk informasi selengkapnya, lihat Undang anggota tim untuk berkolaborasi AWS Pengaturan.
- Beralih antar proyek. Untuk informasi selengkapnya, lihat Beralih antar proyek.
- Kelola metode pembayaran Anda. Untuk informasi selengkapnya, lihat Kelola metode pembayaran Anda di AWS Pengaturan.
- Tingkatkan dari tingkat gratis ke paket berbayar. Untuk informasi selengkapnya, lihat Tingkatkan akun Anda di AWS Pengaturan.
- Kelola batas pengeluaran untuk proyek Anda. Untuk informasi selengkapnya, lihat Buat batas pengeluaran di AWS Pengaturan.
- Lihat informasi penagihan Anda. Untuk informasi selengkapnya, lihat Lihat informasi penagihan Anda di AWS Pengaturan.
- Kelola informasi profil Anda. Lihat informasi selengkapnya di Kelola nama atau nama panggilan Anda di AWS Pengaturan, Ubah alamat email Anda di AWS Pengaturan, dan Mengedit informasi kontak Anda di AWS Pengaturan.
- Kelola pengaturan keamanan dan preferensi masuk Anda. Untuk informasi selengkapnya, lihat Perbarui kata sandi Anda di AWS Pengaturan dan Kelola otentikasi multi-faktor (MFA) di AWS Pengaturan.

Saat Anda mengelola informasi profil atau pengaturan keamanan, Anda akan diarahkan ke ID AWS Builder hub. Anda ID AWS Builder dibuat saat Anda menggunakan Daftar untuk AWS (baru). Untuk informasi lebih lanjut, lihat Apa itu ID AWS Builder? .

Hubungkan alat pengkodean AI

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat menyediakan alat pengkodean AI Anda dengan akses ke proyek Anda dan menginstal Agent Toolkit, yang menggabungkan konfigurasi server AWS MCP dan serangkaian keterampilan agen yang dikuratori. Ini memungkinkan alat pengkodean AI Anda membuat dan mengelola AWS sumber daya atas nama Anda.

Pertimbangan untuk menghubungkan alat pengkodean Anda ke proyek Anda

- Anda dapat menghubungkan alat pengkodean AI ke proyek yang Anda miliki atau proyek yang telah dibagikan dengan Anda.
- Ketika alat pengkodean AI atau agen lokal membuat AWS sumber daya, Anda masih bertanggung jawab untuk mereka. Ini termasuk keamanan yang tepat dari sumber daya Anda sebagaimana ditentukan oleh model tanggung jawab bersama dan biaya apa pun yang mungkin timbul dari sumber daya ini, apakah itu diperhitungkan dalam Paket Gratis atau dibebankan pada Paket Berbayar.
- Anda bertanggung jawab atas tindakan apa pun yang dilakukan alat pengkodean AI Anda atas nama Anda dalam proyek Anda.
- Untuk melihat sumber daya yang dibuat agen Anda, buka konsol layanan untuk layanan tersebut.
- KredenSIAL yang Anda buat adalah untuk digunakan oleh AWS CLI, AWS Tools for PowerShell, dan AWS SDK. Alat eksternal mungkin tidak didukung. Akses ke sumber daya Anda berlaku selama 12 jam. Gunakan perintah berikut untuk memperbarui kredensibilitas Anda:

  ```
  aws login --profile profile-name
  ```

  Ganti *profile-name* dengan nama profil yang Anda pilih selama pengaturan awal. Perintah akan secara otomatis membuka browser default Anda. Anda harus memilih nama proyek Anda untuk menyelesaikan proses login. AWS dapat memperbarui kredensi Anda selama 90 hari. Setelah 90 hari, Anda harus memberikan akses di jendela browser lagi.

Hubungkan alat pengkodean AI Anda ke proyek Anda

Setiap proyek memiliki kumpulan kredensialnya sendiri yang dapat digunakan alat pengkodean AI untuk membuat dan mengelola AWS sumber daya atas nama Anda.

Konsol Manajemen AWS

Untuk menghubungkan alat pengkodean AI Anda ke proyek Anda menggunakan AWS konsol

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih proyek yang ingin Anda akses.
3. Di bilah navigasi di kanan atas, pilih Buat dan kelola infrastruktur cloud.
4. Pilih Gunakan AWS kredensibilitas Anda dengan alat pengkodean AI.
5. Pilih Salin prompt agen dan masukkan di agen pengkodean Anda.

   Ini membuat prompt yang berbagi file pengarahan dengan agen pengkodean AI Anda. File pengarah mengakses skrip AWS yang mengatur koneksi antara kredenSIAL proyek Anda dan agen pengkodean AI Anda.

   Anda akan memasukkan nama profil untuk proyek Anda. Nama profil ini adalah cara alat pengkodean AI Anda mengakses sumber daya Anda.

Use your terminal

Jalankan perintah berikut untuk mengunduh dan ikuti petunjuk penyiapan:

```
curl -fsSL https://github.com/aws/agent-toolkit-for-aws/blob/main/setup-
instructions/setup.md
```

Ketika Anda menggunakan AWS pengalaman baru kami, agen Anda akan menginstal server AWS MCP, dan Anda mendapatkan akses ke keterampilan agen yang dapat digunakan dengan proyek Anda. Anda juga akan mendapatkan file aturan dengan panduan yang disetel untuk pengalaman ini. File aturan juga akan memungkinkan Anda menentukan tingkat bantuan apa yang Anda ingin agen berikan. Berikut ini adalah tingkat bantuan yang didukung:

- Rendah: Saat Anda membangun, keterampilan hanya akan menandai risiko keamanan. Ini tidak akan menyarankan perbaikan atau alternatif untuk arsitektur Anda.

- Sed ang: Saat Anda membangun, keterampilan mungkin mengajukan beberapa pertanyaan klarifikasi jika mendeteksi potensi masalah. Ini tidak akan menyarankan perbaikan atau alternatif untuk arsitektur Anda.
- Tinggi: Saat Anda membangun, keterampilan akan memberikan dukungan tingkat tinggi. Ini akan menyarankan perbaikan atau alternatif untuk arsitektur Anda.

Bekerja dengan beberapa proyek

Setiap proyek memiliki kumpulan kredensialnya sendiri yang dapat digunakan alat pengkodean AI untuk membuat dan mengelola AWS sumber daya atas nama Anda. Anda menggunakan profil untuk mengakses setiap proyek. Profil adalah pengaturan konfigurasi dan file kredensi yang dikelola oleh AWS CLI, dan Anda memberi setiap profil nama unik.

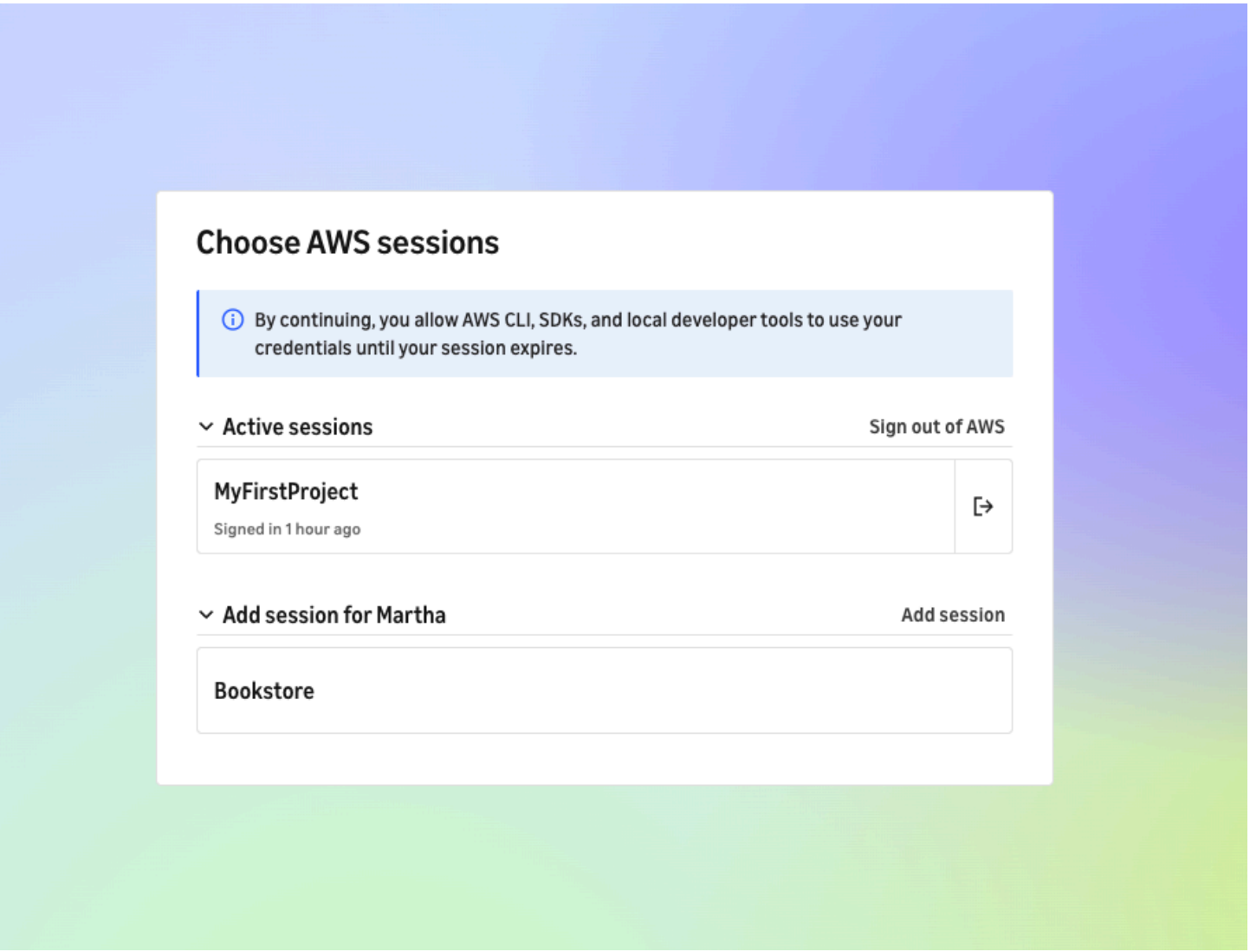
Misalnya, jika proyek pertama Anda adalah `MyFirstProject` dan Anda memilih nama profil `MyFirstProjectProfile` selama penyiapan, Anda dapat mengakses proyek itu dengan masuk ke AWS CLI dengan perintah berikut:

```
aws login --profile MyFirstProjectProfile
```

Jika Anda membuat proyek lain bernama`Bookstore`, Anda dapat mengaksesnya dengan menggunakan skrip pengaturan dan membuat profil`BookstoreProfile`. Kemudian Anda dapat masuk ke AWS CLI dengan perintah berikut:

```
aws login --profile BookstoreProfile
```

Namun, ketika Anda menjalankan salah satu dari perintah ini, Anda harus memilih sesi untuk AWS kredenSIAL Anda di halaman Pilih AWS sesi.



Halaman ini menunjukkan sesi aktif dan sesi yang dapat Anda tambahkan. Sesi mewakili status terautentikasi Anda dengan AWS kredenSIAL Anda, dan ini memberikan kredenSIAL yang sama dengan yang digunakan agen pengkodean AI Anda untuk membuat dan mengelola sumber daya.

Dalam contoh ini, Anda sudah masuk `MyFirstProject` dan belum masuk`Bookstore`. Pada halaman Pilih AWS sesi, Anda dapat melakukan hal berikut:

- Untuk terus menggunakan AWS for`MyFirstProject`, pilih`MyFirstProject`.
- Untuk mengakses`Bookstore`, pilih`Bookstore`.
- Untuk menghapus salah satu sesi saat ini, pilih ikon keluar.
- Untuk mengakses pengguna Akun AWS menggunakan IAM, seperti akun yang Anda buatDaftar untuk AWS (lanjutan), pilih Tam bah sesi.

KredenSIAL yang Anda pilih akan menjadi kredenSIAL yang sama dengan yang digunakan agen pengkodean AI Anda untuk membuat dan mengelola sumber daya. Misalnya, Anda dapat masuk ke AWS CLI dengan perintah berikut:

```
aws login --profile MyFirstProjectProfile
```

Jika Anda kemudian memilih `Bookstore` sesi, alat pengkodean AI Anda akan membuat AWS sumber daya dalam `Bookstore` proyek.

Selalu pilih sesi yang cocok dengan proyek yang terkait dengan profil Anda.

AWS tindakan untuk pemilik proyek

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Ketika Anda memiliki proyek Anda, Anda memiliki kontrol administratif atas proyek Anda. Ini termasuk tugas yang dapat Anda selesaikanGunakan AWS Pengaturan. Anda juga memiliki kemampuan untuk melakukan tindakan root saja. Tindakan ini tidak dapat diselesaikan oleh anggota tim Anda.

Tindakan khusus root saat ini yang dapat Anda lakukan adalah sebagai berikut:

- Mengedit atau menghapus kebijakan bucket S3 yang menolak semua prinsipal. Anda dapat melakukan ini untuk membuka kunci bucket S3 dengan kebijakan bucket yang salah dikonfigurasi.
- Mengedit atau menghapus kebijakan berbasis sumber daya SQS yang menolak semua prinsipal. Anda dapat melakukan ini untuk membuka kunci antrian SQS dengan kebijakan berbasis sumber daya yang salah dikonfigurasi.

Untuk melakukan tindakan hanya root

1. Masuk ke proyek Anda dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol, pilih Manajemen akses root.
3. Untuk tindakan hak istimewa, pilih tindakan istimewa yang ingin Anda lakukan di akun anggota.

- Pilih Hapus kebijakan bucket Amazon S3 untuk menghapus kebijakan bucket yang salah konfigurasi yang menolak semua prinsipal mengakses bucket Amazon S3.

  a. Masukkan URI S3, atau pilih Browse S3 untuk memilih nama dari bucket dalam proyek Anda.

  b. Pilih Hapus kebijakan bucket.

  c. Gunakan konsol Amazon S3 untuk memperbaiki kebijakan bucket setelah menghapus kebijakan yang salah dikonfigurasi. Untuk informasi selengkapnya, lihat Menambahkan kebijakan bucket dengan menggunakan konsol Amazon S3 di Panduan Pengguna Amazon S3.

- Pilih Hapus kebijakan Amazon SQS untuk menghapus kebijakan berbasis sumber daya yang menolak semua prinsipal mengakses antrian Amazon SQS.

  a. Masukkan nama antrian dalam nama antrian SQS.

  b. Pilih H apus kebijakan SQS.

  c. Gunakan konsol Amazon SQS untuk memperbaiki kebijakan antrian setelah menghapus kebijakan yang salah dikonfigurasi. Untuk informasi selengkapnya, lihat Mengonfigurasi kebijakan akses di Amazon SQS di Panduan Pengembang Amazon SQS.

Perbarui kata sandi Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat memperbarui kata sandi Anda di Peng AWS aturan.

Untuk memperbarui kata sandi Anda di AWS Pengaturan

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola keamanan dan masuk.

   Anda akan diarahkan ke profil AWS Builder ID Anda.

3. Untuk O torisasi, pilih Per barui kata sandi.
4. Untuk Kata sandi saat ini, masukkan kata sandi Anda saat ini.
5. Untuk Kata sandi baru, masukkan kata sandi baru.

   AWS mengharuskan kata sandi Anda memenuhi persyaratan berikut:

   - Itu harus memiliki minimal 8 karakter dan maksimum 128 karakter.
   - Ini harus mencakup minimal tiga dari campuran jenis karakter berikut: huruf besar, huruf kecil, angka, dan! @ # $% ^ & * () <> [] {} | _+-= simbol.
6. Untuk Konfirmasi kata sandi baru, masukkan kata sandi baru Anda.
7. Pilih Perbarui.

Kelola otentikasi multi-faktor (MFA) di AWS Pengaturan

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Multi-factor otentikasi (MFA) adalah mekanisme sederhana dan efektif untuk meningkatkan keamanan Anda. Faktor pertama — kata sandi Anda — adalah rahasia yang Anda hafal, juga dikenal sebagai faktor pengetahuan. Faktor lain dapat berupa faktor kepemilikan (sesuatu yang Anda miliki, seperti kunci keamanan) atau faktor warisan (sesuatu yang Anda miliki, seperti pemindaian biometrik). Kami sangat menyarankan Anda mengonfigurasi MFA untuk menambahkan lapisan tambahan untuk akun Anda.

Anda dapat mendaftarkan autentikator bawaan dan juga mendaftarkan kunci keamanan yang Anda simpan di lokasi yang aman secara fisik. Jika Anda tidak dapat menggunakan autentikator bawaan Anda, maka Anda dapat menggunakan kunci keamanan terdaftar Anda. Untuk aplikasi autentikator, Anda juga dapat mengaktifkan fitur pencadangan atau sinkronisasi cloud di aplikasi tersebut. Ini membantu Anda menghindari kehilangan akses ke profil Anda jika Anda kehilangan atau merusak perangkat MFA Anda.

Poin kunci

Ingatlah poin-poin penting berikut saat Anda mendaftar dan mengelola perangkat MFA:

- Kami menyarankan Anda mendaftarkan beberapa perangkat MFA. Jika Anda kehilangan akses ke semua perangkat MFA terdaftar, Anda tidak akan dapat memulihkan akun Anda.
- Kami menyarankan Anda meninjau perangkat MFA terdaftar secara berkala untuk memastikan perangkat tersebut mutakhir dan fungsional. Selain itu, Anda harus menyimpan perangkat tersebut di tempat yang aman secara fisik saat tidak digunakan.
- Jika Anda membuat akun menggunakan Lanjutkan dengan Google, Anda dapat mengaktifkan otentikasi multi-faktor melalui akun Google Anda. Untuk detailnya, lihat Mengaktifkan Verifikasi 2 Langkah.
- Jika Anda membuat akun menggunakan Lanjutkan dengan Apple, autentikasi multi-faktor kemungkinan sudah diaktifkan di Akun Apple Anda. Jika tidak, untuk detail tentang cara mengaktifkannya, lihat Two-factor otentikasi untuk Akun Apple.
- Jika Anda membuat akun menggunakan Lanjutkan dengan GitHub, Anda dapat mengaktifkan otentikasi multi-faktor melalui Akun Anda GitHub . Untuk detailnya, lihat Mengonfigurasi (GitHub) otentikasi dua faktor.
- Jika Anda membuat akun menggunakan Lanjutkan dengan Amazon, Anda dapat mengaktifkan otentikasi multi-faktor melalui Akun Amazon Anda. Untuk detailnya, lihat Apa itu Two-Step Verifikasi? .

Jenis MFA yang tersedia untuk baru kami AWS pengalaman

AWS Pengalaman baru kami mendukung jenis perangkat otentikasi multi-faktor (MFA) berikut.

Otentikator FIDO2

FIDO2 adalah standar yang mencakup CTAP2 dan WebAuthndan didasarkan pada kriptografi kunci publik. Kredensi FIDO tahan terhadap phishing karena unik untuk situs web tempat kredensialnya dibuat. AWS

AWS mendukung dua faktor bentuk yang paling umum untuk otentikator FIDO: autentikator bawaan dan kunci keamanan. Lihat di bawah untuk informasi lebih lanjut tentang jenis otentikator FIDO yang paling umum.

Built-in autentikator

Beberapa perangkat memiliki autentikator bawaan, seperti TouchID aktif MacBook atau kamera Windows Hello-compatible . Jika perangkat Anda kompatibel dengan protokol FIDO, termasuk

WebAuthn, Anda dapat menggunakan sidik jari atau wajah Anda sebagai faktor kedua. Untuk informasi selengkapnya, lihat Otentikasi FIDO.

Kunci keamanan

Anda dapat membeli USB FIDO2-compatible eksternal, BLE, atau kunci NFC-connected keamanan. Saat Anda diminta untuk perangkat MFA, ketuk sensor tombol. YubiKey atau Feitian membuat perangkat yang kompatibel. Untuk daftar semua kunci keamanan yang kompatibel, lihat Produk Bersertifikat FIDO.

Pengelola kata sandi, penyedia kunci sandi, dan otentikator FIDO lainnya

Beberapa penyedia pihak ketiga mendukung otentikasi FIDO dalam aplikasi seluler, sebagai fitur dalam pengelola kata sandi, kartu pintar dengan mode FIDO, dan faktor bentuk lainnya. FIDO-compatible Perangkat ini dapat bekerja dengan IAM Identity Center, tetapi kami menyarankan Anda menguji autentikator FIDO sendiri sebelum mengaktifkan opsi ini untuk MFA.

> **Note**
>
> Beberapa autentikator FIDO dapat membuat kredensil FIDO yang dapat ditemukan yang dikenal sebagai kunci sandi. Passkey mungkin terikat ke perangkat yang membuatnya, atau mereka dapat disinkronkan dan dicadangkan ke cloud. Misalnya, Anda dapat mendaftarkan kunci sandi menggunakan Apple Touch ID di Macbook yang didukung, lalu masuk ke situs dari laptop Windows menggunakan Google Chrome dengan kunci sandi Anda di iCloud dengan mengikuti petunjuk di layar saat masuk. Untuk informasi selengkapnya tentang perangkat mana yang mendukung kunci sandi yang dapat disinkronkan dan interoperabilitas kunci sandi saat ini antara sistem operasi dan browser, lihat Dukungan Perangkat di passkeys.dev, sumber daya yang dikelola oleh FIDO Alliance And World Wide Web Consortium (W3C).

Aplikasi Authenticator

Aplikasi Authenticator adalah one-time password (OTP) berbasis third party authenticator. Anda dapat menggunakan aplikasi autentikator yang diinstal pada perangkat seluler atau tablet Anda sebagai perangkat MFA resmi. Aplikasi autentikator pihak ketiga harus sesuai dengan RFC 6238, yang merupakan algoritma kata sandi satu kali berbasis waktu (TOTP) berbasis waktu berbasis standar yang mampu menghasilkan kode otentikasi enam digit.

Saat diminta untuk MFA, Anda harus memasukkan kode yang valid dari aplikasi autentikator Anda di dalam kotak input yang disajikan. Setiap perangkat MFA yang ditetapkan ke pengguna harus unik. Dua aplikasi autentikator dapat didaftarkan untuk setiap pengguna tertentu.

Anda dapat memilih dari aplikasi otentikator pihak ketiga terkenal berikut. Namun, TOTP-compliant aplikasi apa pun berfungsi dengan AWS Builder ID MFA.

Sistem operasi	Aplikasi autentikator yang diuji
Android	1 Kata Sandi, Authy, Duo Mobile, Microsoft Authenticator,Google Authenticator
iOS	1 Kata Sandi, Authy, Duo Mobile, Microsoft Authenticator,Google Authenticator

Daftarkan perangkat MFA Anda

> **Note**
>
> Setelah mendaftar ke MFA, keluar, lalu masuk di perangkat yang sama, Anda mungkin tidak akan diminta untuk MFA di perangkat tepercaya.

Untuk mendaftarkan perangkat MFA Anda menggunakan aplikasi autentikator

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola keamanan dan masuk.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
3. Pada halaman Keamanan, pilih Daftarkan perangkat.
4. Pada halaman Daftarkan perangkat MFA, pilih aplikasi Authenticator.
5. AWS Builder ID mengoperasikan dan menampilkan informasi konfigurasi, termasuk grafik kode QR. Grafik adalah representasi dari “kunci konfigurasi rahasia” yang tersedia untuk entri manual di aplikasi otentikator yang tidak mendukung kode QR.
6. Buka aplikasi autentikator Anda. Untuk daftar aplikasi, lihatAplikasi Authenticator.

Jika aplikasi autentikator mendukung beberapa perangkat atau akun MFA, pilih opsi untuk membuat perangkat atau akun MFA baru.

7. Tentukan apakah aplikasi MFA mendukung kode QR, lalu lakukan salah satu hal berikut di halaman Siapkan aplikasi autentikator Anda:

   1. Pilih Tampilkan kode QR, lalu gunakan aplikasi untuk memindai kode QR. Misalnya, Anda dapat memilih ikon kamera atau memilih opsi yang mirip dengan kode Pindai. Kemudian gunakan kamera perangkat untuk memindai kode.
   2. Pilih Tampilkan kunci rahasia, lalu masukkan kunci rahasia itu ke aplikasi MFA Anda.

   Setelah selesai, aplikasi autentikator Anda akan menghasilkan dan menampilkan kata sandi satu kali.

8. Di kotak kode Authenticator, masukkan kata sandi satu kali yang saat ini muncul di aplikasi autentikator Anda. Pilih Tugaskan MFA.

   > **Important**
   >
   > Kirim permintaan Anda segera setelah membuat kode. Jika Anda membuat kode dan kemudian menunggu terlalu lama untuk mengirimkan permintaan, perangkat MFA berhasil dikaitkan dengan ID AWS Builder Anda, tetapi perangkat MFA tidak sinkron. Hal ini terjadi karena kata sandi sekali pakai berbasis waktu (TOTP) kedaluwarsa setelah periode waktu yang singkat. Jika ini terjadi, Anda dapat menyinkronisasi ulang perangkat. Untuk informasi selengkapnya, lihat *I get the message 'An unexpected error has occurred' when I try to register or sign in with an authenticator app*.

9. Untuk memberi perangkat Anda nama yang ramah di AWS Builder ID, pilih Ganti nama. Nama ini membantu Anda membedakan perangkat ini dari perangkat lain yang Anda daftarkan.

Perangkat MFA sekarang siap digunakan dengan AWS Pengaturan, proyek Anda, dan AWS Builder ID.

Daftarkan kunci keamanan sebagai perangkat MFA Anda

Untuk mendaftarkan perangkat MFA Anda menggunakan kunci keamanan

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola keamanan dan masuk.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
3. Pada halaman Keamanan, pilih Daftarkan perangkat.
4. Pada halaman Daftarkan perangkat MFA, pilih Kunci keamanan.
5. Pastikan kunci keamanan Anda diaktifkan. Jika Anda menggunakan kunci keamanan fisik terpisah, sambungkan ke komputer Anda.
6. Ikuti instruksi di layar Anda. Pengalaman Anda bervariasi berdasarkan sistem operasi dan browser Anda.
7. Untuk memberi perangkat Anda nama yang ramah di AWS Builder ID, pilih Ganti nama. Nama ini membantu Anda membedakan perangkat ini dari perangkat lain yang Anda daftarkan.

Perangkat MFA sekarang siap digunakan dengan AWS Pengaturan, proyek Anda, dan AWS Builder ID.

Ganti nama perangkat MFA Anda

Untuk mengganti nama perangkat MFA Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola keamanan dan masuk.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
3. Pilih Keamanan. Ketika Anda tiba di halaman, Anda melihat bahwa Ganti nama berwarna abu-abu.
4. Pilih perangkat MFA yang ingin Anda ubah. Ini memungkinkan Anda untuk memilih Ganti nama. Kemudian kotak dialog muncul.
5. Pada prompt yang terbuka, masukkan nama baru di nama perangkat MFA, dan pilih Ganti nama. Perangkat yang diganti namanya muncul di bawah perangkat Multi-factor otentikasi (MFA).

Hapus perangkat MFA Anda

Kami menyarankan Anda menyimpan dua atau lebih perangkat MFA aktif. Untuk menonaktifkan otentikasi multi-faktor, hapus semua perangkat MFA terdaftar dari profil Anda.

Untuk menghapus perangkat MFA

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola keamanan dan masuk.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
3. Pada halaman Keamanan, pilih perangkat MFA yang ingin Anda ubah dan pilih Hapus.
4. Di perangkat Hapus MFA? modal, ikuti petunjuk untuk menghapus perangkat Anda.
5. Pilih Hapus.

Perangkat yang dihapus tidak lagi muncul di bawah perangkat Multi-factor otentikasi (MFA).

Hapus semua sesi di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat menghapus semua sesi di seluruh perangkat di Peng AWS aturan. Jika ada perangkat yang tidak Anda kenali, ubah kata sandi Anda dan hapus semua sesi.

Untuk menghapus semua sesi

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola keamanan dan masuk.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
3. Untuk Perangkat yang masuk, pilih H apus semua sesi.
4. Konfirmasikan pilihan Anda dan pilih Hapus semua sesi.

Anda akan keluar dari Peng AWS aturan.

Kelola nama atau nama panggilan Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat mengubah nama Anda kapan saja. Semua anggota tim dapat melihat nama Anda, dan jika Anda telah meningkatkan ke Paket Berbayar, ini adalah nama yang muncul di informasi penagihan Anda. Jika Anda mendaftar AWS di India, nama Anda harus sama persis dengan nama yang muncul pada dokumen yang akan Anda gunakan untuk verifikasi pelanggan.

Saat Anda mengubah nama Anda, Anda mengubah nama di ID AWS Builder Anda. Ini akan memengaruhi nama Anda di Peng AWS aturan, ID AWS Pembuat, dan AWS sumber daya apa pun yang Anda akses langsung melalui ID AWS Pembuat.

Nama Anda adalah bagaimana Anda disebut dalam alat dan layanan saat berinteraksi dengan orang lain. Nama Panggilan Anda menunjukkan bagaimana Anda ingin dikenal oleh AWS, teman, dan orang lain yang bekerja sama dengan Anda.

Untuk mengubah nama atau nama panggilan Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil.
3. Untuk Info Profil, pilih Kel ola profil.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
4. Untuk informasi profil, pilih Edit.
5. (Opsional) Untuk Nama, masukkan nama baru.
6. (Opsional) Untuk Nama panggilan, masukkan nama panggilan baru.
7. Pilih Simpan perubahan.

Ubah alamat email Anda di AWS Pengaturan

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat mengubah email Anda di AWS Pengaturan. Ketika Anda mengubah email Anda, email Anda sebelumnya akan dipisahkan dari AWS profil Anda dan AWS Builder ID. Anda tidak akan dapat menggunakan email itu untuk mengakses proyek apa pun di AWS Pengaturan, tetapi Anda dapat menggunakan email itu untuk mendaftar AWS lagi.

Alamat email Anda dibagikan dengan anggota tim saat Anda memberi mereka akses ke proyek Anda.

Untuk mengubah email Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola profil.
3. Untuk info Profil, pilih Kelola profil.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
4. Untuk informasi Kontak, pilih Edit.
5. Untuk alamat Email, masukkan alamat email baru dan pilih Verifikasi email. Kami akan mengirimkan kode verifikasi untuk alamat email baru Anda. Itu akan Anda masukkan di kotak popup Verifikasi email.
6. Untuk kode Verifikasi, masukkan kode verifikasi yang kami kirimkan ke email baru Anda.
7. Pilih Verifikasi.

Mengedit informasi kontak Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat mengedit nomor telepon atau alamat yang terkait dengan Peng AWS aturan. Ketika Anda mengubah nilai-nilai ini, nilai-nilai tersebut dapat memengaruhi kewajiban pajak.

Untuk mengedit informasi kontak Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil.
3. Untuk informasi kontak, pilih Edit.
4. Masukkan informasi kontak baru.
5. Pilih Simpan.

Memilih tidak menggunakan konten Anda untuk peningkatan layanan di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

AWS Layanan AI dapat menggunakan dan menyimpan konten pelanggan untuk peningkatan layanan, seperti memperbaiki masalah operasional, mengevaluasi kinerja layanan, debugging, atau pelatihan model. Untuk tujuan ini, kami dapat menyimpan konten tersebut Wilayah AWS di luar Wilayah AWS tempat Anda menggunakan layanan. Anda dapat memilih keluar dari penggunaan konten Anda untuk peningkatan layanan melalui Peng AWS aturan. Efek dari memilih keluar adalah AWS melampirkan kebijakan opt-out layanan AI ke AWS organisasi Anda. Untuk informasi selengkapnya tentang kebijakan opt-out, lihat dokumentasi kebijakan opt-out layanan AI.

Memilih untuk memilih keluar dari semua layanan akan memilih semua proyek Anda keluar dari peningkatan layanan menggunakan konten Anda untuk layanan AI yang didukung saat ini dan di masa mendatang yang didukung oleh kebijakan opt-out layanan AI.

Langkah-langkah tambahan diperlukan untuk memilih keluar dari Amazon Monitron. Untuk informasi lebih lanjut, lihat Ketentuan Layanan AWS. Hanya pemilik proyek yang dapat memilih keluar dari penggunaan data oleh layanan AWS AI.

Untuk memilih keluar dari penggunaan data oleh AWS Layanan AI

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Project.
3. Untuk Ikh tisar , pilih Tindakan, lalu pilih Memilih keluar dari penggunaan data oleh layanan AWS AI.
4. Konfirmasikan pilihan Anda dan pilih Opt Out.

Minta Anda AWS Data ID Pembangun

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat meminta dan melihat informasi pribadi yang terkait dengan ID AWS Builder Anda dan AWS aplikasi serta layanan yang Anda akses dengan ID AWS Builder Anda. Kami akan memproses permintaan Anda dalam waktu 30 hari dan memberi tahu Anda ketika data Anda siap. Sementara permintaan data Anda tertunda, Anda tidak dapat menutup AWS profil Anda. Anda masih dapat menutup proyek atau organisasi yang memiliki semua proyek Anda.

Untuk informasi lebih lanjut tentang menggunakan hak subjek data Anda, termasuk untuk informasi pribadi yang diberikan sehubungan dengan AWS situs web, aplikasi, produk, layanan, acara, dan pengalaman lain, lihat AWS Privasi.

Untuk meminta data Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil.
3. Pilih Kelola profil.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
4. Pilih Privasi & data.
5. Pilih untuk meminta data Builder ID atau AWS data Anda.

Pesan konfirmasi hijau muncul di bagian atas halaman bahwa kami menerima permintaan Anda dan akan menyelesaikannya dalam waktu 30 hari.

6. Ketika Anda menerima email dari kami bahwa permintaan telah diproses, navigasikan kembali ke halaman Privasi & data profil ID AWS Pembangun Anda. Pilih tombol yang baru tersedia Unduh arsip ZIP dengan data Anda.

Sementara permintaan data Anda tertunda, Anda tidak akan dapat menghapus ID AWS Builder Anda.

Buat proyek di AWS Pengaturan

> ⚠ Warning
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Sebuah proyek berisi satu Akun AWS tempat Anda membuat AWS sumber daya. Sebuah proyek juga mencakup pengaturan untuk berbagi dengan kolaborator lain. Sumber AWS daya yang Anda buat harus mewakili aplikasi atau serangkaian kasus penggunaan terkait. Satu proyek dapat menjangkau lingkungan pengembangan dan produksi aplikasi Anda. Misalnya, Anda dapat membuat proyek bernama Bookstore yang menyimpan sumber daya untuk aplikasi toko buku termasuk database, sumber daya komputasi, dan penyimpanan.

Anda dapat berbagi proyek ini dengan anggota tim lain, dan mereka dapat membangun dan mengelola sumber daya untuk aplikasi toko buku.

Setiap proyek memiliki kontrol biaya sendiri berdasarkan sumber daya dalam akun. Jika Anda menggunakan paket berbayar, Anda dapat mengonfigurasi batas pengeluaran di AWS Pengaturan untuk setiap proyek. Untuk informasi selengkapnya, lihat Buat batas pengeluaran di AWS Pengaturan. Sebagai pemilik proyek, Anda bertanggung jawab atas faktur bulanan untuk biaya penggunaan dan biaya berulang.

Pertimbangan untuk membuat proyek

- Anda dapat mengakses proyek yang tidak Anda miliki sebagai anggota tim.

- Setiap nama proyek harus unik untuk proyek Anda. Proyek yang dimiliki oleh anggota tim lain dapat memiliki nama yang sama.
- Nama proyek dapat berisi karakter valid berikut: a-z,, 0-9 A-Z, dan periode (.).
- Saat Anda membuat proyek, AWS tetapkan ke suatu wilayah—US East (Ohio) (), Eropa (Stockholm`us-east-2`) (), atau Asia Pasifik (Sydney`eu-north-1`) (`ap-southeast-2`) — berdasarkan negara di alamat kontak Anda—baik Amerika Serikat, Eropa, atau Asia Pasifik. Sumber daya Regional apa pun yang Anda buat akan di-host di Wilayah tersebut. Untuk informasi selengkapnya, lihat Wilayah AWS untuk proyek Anda.

Untuk membuat proyek

Untuk membuat proyek

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Project.
3. Pilih Buat proyek.
4. Untuk nama Proyek, masukkan nama deskriptif untuk proyek Anda.

   Nama ini dibagikan dengan anggota tim saat Anda mengundang mereka untuk berkolaborasi.
5. Pilih Buat.

Dibutuhkan beberapa detik untuk membuat proyek Anda. Ketika proyek Anda tersedia, Anda dapat memilih proyek dan mengakses Konsol Manajemen AWS untuk mulai membangun.

Jika Anda sudah menyiapkan alat pengkodean AI untuk berinteraksi dengan Anda Akun AWS, Anda dapat memintanya untuk membuat sumber daya di proyek baru Anda.

Gunakan contoh petunjuk untuk alat pengkodean AI Anda untuk memulai:

```
What is the Region for my project test project?
```

```
Create a hello world Lambda function in my project test project.
```

```
Create an S3 bucket in my project test project.
```

Wilayah AWS untuk proyek Anda

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Saat Anda membuat proyek, tetapkan AWS proyek ke wilayah—AS Timur (Ohio) (`us-east-2`), Eropa (Stockholm) (`eu-north-1`), atau Asia Pasifik (Sydney) (`ap-southeast-2`) —berdasarkan negara di alamat kontak Anda—baik Amerika Serikat, Eropa, atau Asia Pasifik. Setiap sumber daya Regional yang Anda buat akan di-host di Wilayah tersebut.

Berikut ini adalah pertimbangan untuk yang dipilih Wilayah AWS untuk akun Anda:

- Jika Anda mengubah informasi kontak Anda di Peng AWS aturan, Wilayah yang Anda pilih tidak akan berubah. Jika Anda perlu mengakses Wilayah tertentu, gunakan Daftar untuk AWS (lanjutan). Anda juga dapat mengaktifkan fitur lanjutan untuk akun Anda untuk memilih Wilayah yang berbeda.
- AWS dapat memperkenalkan Wilayah tambahan yang didukung, tetapi itu hanya akan tersedia untuk pendaftaran baru. Untuk melihat Wilayah terbaru yang didukung per 18 Agustus 2026, lihat tabel di bawah ini. Jika Anda sudah memiliki proyek, Anda dapat menemukan Wilayah yang Anda pilih di Peng AWS aturan.
- Layanan global tersedia dengan proyek Anda. Layanan ini diakses melalui satu wilayah yang mungkin berbeda dari wilayah asal Anda. Untuk informasi selengkapnya, lihat B AWS atas Isolasi Kesalahan. Selain itu, ada beberapa layanan yang tersedia di Wilayah tertentu. Di dalam Konsol Manajemen AWS, Anda dapat melihat layanan ini di Wilayah tertentu, tetapi Anda akan kembali ke Wilayah yang dipilih saat menavigasi ke layanan lain.
- Jika Anda menggunakan Amazon Bedrock, Anda dapat menggunakan API yang tidak membuat sumber daya di semua komersial Wilayah AWS yang diaktifkan secara default.
- Jika Anda menggunakan CloudFront, fitur tertentu yang akan membuat sumber daya di luar Wilayah yang dipilih tidak tersedia. Ini termasuk menggunakan AWS WAF dengan CloudFront.
- Beberapa CloudTrail peristiwa yang melibatkan layanan global dicatat di Wilayah tempat layanan global beroperasi. Anda memiliki akses ke acara-acara ini.
- AWS WAF dan Amazon CloudWatch Log tersedia di AS Timur (Virginia Utara) (`us-east-1`).

Anda dapat menemukan Wilayah yang dipilih untuk semua proyek di akun Anda dengan menggunakan Peng AWS aturan. Di Konsol Manajemen AWS, sebagian besar konsol layanan di-host di Wilayah tempat Anda berada, termasuk Bedrock dan SageMaker. Jika Anda pernah melihat konsol layanan dari layanan global, konsol secara otomatis merutekan semua panggilan API Anda ke Wilayah yang sesuai untuk layanan global.

Temukan yang dipilih Wilayah AWS untuk proyek Anda

Sebagai praktik terbaik, kami sarankan Anda selalu mengkonfirmasi Wilayah AWS untuk proyek Anda sebelum Anda membuat AWS sumber daya apa pun.

Untuk menemukan yang dipilih Wilayah AWS untuk proyek Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Project.
3. Di bagian I khtisar, pilih Info Tambahan.

   Dalam tampilan ini, Anda juga dapat menemukan Akun AWS ID yang terkait dengan proyek Anda.
4. Untuk Wilayah, Anda akan melihat proyek Wilayah AWS Anda telah disediakan.

Saat Anda membuat AWS sumber daya Regional di salah satu proyek Anda, Nama Sumber Daya Amazon dari sumber daya ini akan menyertakan ini Wilayah AWS.

Negara-negara di mana sumber daya Regional disediakan di AS Timur (Ohio) (`us-` east-2)

Nama negara	Kode negara
Antigua dan Barbuda	AG
Argentina	AR
Bahama	BBS
Barbados	BB
Belize	BZ

Nama negara	Kode negara
Bolivia	BO
Brazil	BR
Kanada	CA
Chili	CL
Kolombia	CO
Kosta Rika	CR
Dominika	DM
Republik Dominika	LAKUKAN
Ekuador	EC
El Salvador	SV
Grenada	GD
Guatemala	GT
Guyana	GY
Haiti	IT
Honduras	NO
Jamaika	JM
Meksiko	MX
Nikaragua	NO
Panama	PA
Paraguay	PY

Nama negara	Kode negara
Peru	PE
Saint Kitts dan Nevis	KN
Saint Lucia	LC
Saint Vincent dan Grenadines	VC
Suriname	SR
Trinidad dan Tobago	TW
Amerika Serikat	AS
Uruguay	MY
Venezuela	A
Anguilla	AI
Aruba	AW
Bermuda	BM
Bonaire, Saint Eustatius dan Saba	BQ
Kepulauan Virgin Inggris	VG
Kepulauan Cayman	KY
Curaçao	CW
Kepulauan Falkland	FK
Guyana Prancis	GF
Guadeloupe	DOKTER UMUM
Martinik	MQ

Nama negara	Kode negara
Montserrat	MS
Puerto Riko	PR
Saint Barthélemy	BL
Saint Martin	MF
Saint Pierre dan Miquelon	PM
Sint Maarten	SX
Kepulauan Turks dan Caicos	TC
U.S. Kepulauan Virgin	VI

Negara-negara tempat sumber daya Regional disediakan di Asia Pasifik (Sydney) (**ap-** southeast-2)

Nama negara	Kode negara
Afghanistan	OLEH
Australia	AU
Bangladesh	BD
Bhutan	BT
Brunei	BN
Kamboja	KH
China	CN
Timor Timur () Timor-Leste	TL

Nama negara	Kode negara
Fiji	FJ
Hong Kong	HK
India	DI DALAM
Indonesia	ID
Jepang	JP
Kazakstan	KZ
Kiribati	KI
Kirgistan	KG
Laos	LA
Macau	MO
Malaysia	MILIKKU
Maladewa	MV
Kepulauan Marshall	MH
Mikronesia	FM
Mongolia	MN
Myanmar	MM
Nauru	NO
Nepal	NP
Selandia Baru	NZ
Pakistan	PK

Nama negara	Kode negara
Palau	PW
Papua Nugini	PG
Filipina	PH
Samoa	WS
Singapura	SG
Kepulauan Solomon	SB
Korea Selatan	KR
Sri Lanka	LK
Taiwan	TW
Tajikistan	TJ
Thailand	TH
Tonga	KE
Turkmenistan	TM
Tuvalu	TV
Uzbekistan	IS
Vanuatu	VU
Vietnam	NO
Samoa Amerika	AS
Pulau Natal	CX
Kepulauan Cocos (Keeling)	CC

Nama negara	Kode negara
Kepulauan Cook	CK
Polinesia Perancis	PF
Guam	GU
Pulau Heard dan McDonald Kepulauan	HM
Kaledonia Baru	NC
Niue	NU
Pulau Norfolk	NF
Kepulauan Mariana Utara	MP
Kepulauan Pitcairn	PN
Tokelau	TK
U.S. Kepulauan Terluar Kecil	UM
Wallis dan Futuna	WF

Negara-negara di mana sumber daya regional disediakan di Eropa (Stockholm) (**eu-** utara-1)

Nama negara	Kode negara
Albania	AL
Aljazair	DZ
Andorra	AD
Angola	EL

Nama negara	Kode negara
Armenia	SAYA
Austria	DI
Azerbaijan	AZ
Bahrain	BH
Belarus	OLEH
Belgium	MENJADI
Benin	BJ
Bosnia dan Herzegovina	BA
Botswana	BLACK
Bulgaria	BG
Burkina Faso	BFF
Burundi	BI
Tanjung Verde	CV
Kamerun	CM
Republik Afrika Tengah	LIH
Chad	TD
Komoro	KM
Kongo (Brazzaville)	CG
Kongo (DRC)	CD
Pantai Gading	CI

Nama negara	Kode negara
Croatia	SDM
Cyprus	CY
Czech Republic	CZ
Denmark	DK
Djibouti	DJ
Mesir	MISALNYA
Guinea Khatulistiwa	GQ
Eritrea	ER
Estonia	EE
Swaziland	SZ
Etiopia	ET
Finland	FI
France	FR
Gabon	GA
Gambia	GM
Georgia	GE
Germany	DARI
Ghana	GH
Greece	GR
Guinea	GN

Nama negara	Kode negara
Guinea-Bissau	GW
Hungary	IL
Islandia	ADALAH
Irak	IQ
Ireland	YAITU
Israel	IL
Italy	ITU
Yordania	JO
Kenya	LE
Kosovo	XK
Kuwait	KW
Latvia	LV
Libanon	LB
Lesotho	LS
Liberia	LR
Libya	LY
Liechtenstein	IL
Lithuania	LT
Luxembourg	IL
Madagaskar	MG

Nama negara	Kode negara
Malawi	MW
Mali	MILILITRI
Malta	MT
Mauritania	TN
Mauritius	MU
Moldova	MD
Monako	MC
Montenegro	SAYA
Maroko	MA
Mozambik	MZ
Namibia	TA
Netherlands	NL
Niger	NE
Nigeria	NG
Makedonia Utara	MK
Norwegia	TIDAK
Oman	OM
Palestina	PS
Poland	PL
Portugal	PT

Nama negara	Kode negara
Qatar	QA
Romania	RO
Rusia	RU
Rwanda	RW
San Marino	SM
Sao Tome dan Principe	ST
Arab Saudi	SA
Senegal	SN
Serbia	RS
Seychelles	SC
Sierra Leone	SL
Slovakia	SK
Slovenia	SI
Somalia	JADI
Afrika Selatan	FOR
Sudan Selatan	SS
Spain	ES
Sweden	SE
Swiss	CH
Tanzania	TZ

Nama negara	Kode negara
Togo	TG
Tunisia	TW
Turki	TR
Uganda	UG
Ukraina	A
Uni Emirat Arab	AE
Britania Raya	GB
Kota Vatikan	VA
Yaman	YOU
Zambia	ZM
Zimbabwe	ZW
Kepulauan Åland	KAPAK
Antartika	AQ
Pulau Bouvet	BV
Wilayah Samudra Hindia Britania	IO
Kepulauan Faroe	FOR
Wilayah Selatan Prancis	TF
Gibraltar	DON'T
Greenland	GL
Guernsey	GG

Nama negara	Kode negara
Pulau Man	IM
Jersey	IS
Mayotte	IT
Reunion	KEMBALI
Saint Helena	SH
Georgia Selatan dan Kepulauan Sandwich Selatan	GS
Svalbard dan Jan Mayen	SJ
Sahara Barat	EH

Kebijakan terkelola untuk organisasi Anda

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Saat Anda menggunakan AWS pengalaman baru kami, AWS mengelola kebijakan manajemen organisasi termasuk kebijakan pengendalian sumber daya (RCP) dan kebijakan kontrol layanan (SCP). Kontrol pelindung ini mencegah pemilik proyek atau anggota tim melakukan tindakan yang akan menghambat default yang AWS telah ditentukan sebelumnya untuk membantu Anda membangun dan mengembangkan dengan cepat.

Kebijakan kontrol layanan untuk proyek

Berikut ini adalah kebijakan kontrol layanan untuk semua pengguna dalam proyek dan tidak dapat diubah:

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "BlockOrgEscape",
      "Effect" : "Deny",
      "Action" : [
        "account:CloseAccount",
        "organizations:AcceptHandshake",
        "organizations:LeaveOrganization",
        "sso:CreateInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProtectManagedRoles",
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:UntagRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : "arn:*:iam::*:role/managed/*",
      "Condition" : {
        "StringNotLike" : {
          "aws:PrincipalArn" : "arn:*:iam::*:role/managed/
AWSManagedAccountManagementAccessRole"
        }
      }
    }
  ]
}
```

Kebijakan ini tidak dihapus saat Anda mengaktifkan fitur lanjutan. Untuk informasi selengkapnya, lihat Aktifkan lanjutan AWS fitur.

Setelah Anda mengaktifkan fitur lanjutan, kebijakan ini tetap melekat pada akar organisasi Anda, sehingga berlaku untuk setiap akun anggota, termasuk akun yang Anda buat atau undang nanti.

Selain itu, kami menerapkan kebijakan kontrol layanan berikut untuk semua pengguna dalam proyek untuk membatasi modifikasi tertentu pada proyek Anda yang tidak didukung atau harus diselesaikan di AWS Pengaturan:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BlockAccountManagementAPIs",
      "Effect" : "Deny",
      "Action" : [
        "account:AcceptPrimaryEmailUpdate",
        "account:DeleteAlternateContact",
        "account:DisableRegion",
        "account:EnableRegion",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetRegionOptStatus",
        "account:PutAccountName",
        "account:PutAlternateContact",
        "account:PutContactInformation",
        "account:StartPrimaryEmailUpdate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyBillingOperations",
      "Effect" : "Deny",
      "Action" : "billing:*",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotificationContactsOperations",
      "Effect" : "Deny",
      "Action" : "notifications-contacts:*",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyRestrictedNotificationOperations",
```

```
      "Effect" : "Deny",
      "Action" : [
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
        "notifications:AssociateOrganizationalUnit",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:DisassociateOrganizationalUnit",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListMemberAccounts",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "notifications:PutFeatureOptInStatus",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyRoleManagerDisablement",
      "Effect" : "Deny",
      "Action" : "iam:PutAccountProperties",
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AccountPropertyNamespaces" : "RoleManager"
        }
      }
    }
  ]
}
```

Kebijakan ini dihapus saat Anda mengaktifkan fitur lanjutan. Untuk informasi selengkapnya, lihat Aktifkan lanjutan AWS fitur.

Menghapus kebijakan ini tidak memungkinkan Anda memperbarui alamat email pengguna root dari akun proyek. Untuk informasi selengkapnya, lihat Akun proyek setelah Anda mengaktifkan fitur lanjutan.

Selain itu, kami juga menerapkan kebijakan kontrol layanan berikut untuk semua pengguna dalam proyek untuk membatasi Wilayah AWS untuk memungkinkan dukungan untuk layanan partisi, tergantung pada Anda: *selected-region*

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
```

```
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "budgets:*",
        "ce:*",
        "chatbot:*",
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "consoleapp:*",
        "cost-optimization-hub:*",
        "ec2:DescribeRegions",
        "ecr-public:*",
        "freetier:*",
        "health:*",
        "iam:*",
        "identitystore-auth:*",
        "identitystore:*",
        "invoicing:*",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lightsail:AttachCertificateToDistribution",
        "lightsail:CreateCertificate",
        "lightsail:CreateContactMethod",
        "lightsail:CreateDistribution",
        "lightsail:CreateDomain",
        "lightsail:CreateDomainEntry",
        "lightsail:DeleteAlarm",
        "lightsail:DeleteCertificate",
        "lightsail:DeleteContactMethod",
        "lightsail:DeleteDistribution",
        "lightsail:DeleteDomain",
        "lightsail:DeleteDomainEntry",
        "lightsail:DetachCertificateFromDistribution",
        "lightsail:Get*",
```

```
        "lightsail:IsVpcPeered",
        "lightsail:PutAlarm",
        "lightsail:ResetDistributionCache",
        "lightsail:SendContactMethodVerification",
        "lightsail:SetIpAddressType",
        "lightsail:TagResource",
        "lightsail:TestAlarm",
        "lightsail:UntagResource",
        "lightsail:UpdateDistribution",
        "lightsail:UpdateDistributionBundle",
        "lightsail:UpdateDomainEntry",
        "logs:*",
        "managedblockchain-query:*",
        "managedblockchain:*",
        "mapcredits:*",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:ListManagedNotificationChildEvents",
        "notifications:ListManagedNotificationConfigurations",
        "notifications:ListManagedNotificationEvents",
        "organizations:*",
        "pricing:*",
        "q:*",
        "route53:*",
        "route53domains:*",
        "route53globalresolver:*",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "servicequotas:*",
        "signin:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "sts:*",
        "support:*",
        "tax:*",
        "trustedadvisor:*",
        "uxc:*",
        "waf:*",
        "wafv2:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "DenyUsEast1WafResourceAssociation",
      "Effect" : "Deny",
      "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "UsWest2Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "health:*",
        "identitystore-auth:*",
        "identitystore:*",
        "kms:Decrypt",
```

```
        "kms:DescribeKey",
        "kms:ListAliases",
        "networkmanager-chat:*",
        "networkmanager:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "servicequotas:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "support:*",
        "trustedadvisor:*",
        "uxc:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-west-2"
        }
      }
    },
    {
      "Sid" : "RegionFloor",
      "Effect" : "Deny",
      "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
```

```
          "aws:RequestedRegion" : [
            "unspecified",
            "us-east-1",
            "selected-region",
            "us-west-2"
          ]
        }
      }
    }
  ]
}
```

Setelah Anda mengaktifkan fitur-fitur lanjutan, kebijakan kontrol layanan berikut diterapkan ke akun Anda:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "a4b:*",
        "access-analyzer:*",
        "account-access:*",
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace-management:*",
        "aws-marketplace:*",
        "aws-portal:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
```

```
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "billing:*",
        "billingconductor:*",
        "budgets:*",
        "builderid:*",
        "ce:*",
        "chatbot:*",
        "chime:*",
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "compute-optimizer:*",
        "config:*",
        "consoleapp:*",
        "consolidatedbilling:*",
        "cost-optimization-hub:*",
        "cur:*",
        "datapipeline:GetAccountLimits",
        "devicefarm:*",
        "directconnect:*",
        "ec2:DescribeRegions",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnGateways",
        "ecr-public:*",
        "fms:*",
        "freetier:*",
        "globalaccelerator:*",
        "health:*",
        "iam:*",
        "identitystore-auth:*",
        "identitystore:*",
        "importexport:*",
        "invoicing:*",
        "iq:*",
        "kms:*",
        "license-manager:ListReceivedLicenses",
```

```
        "lightsail:AttachCertificateToDistribution",
        "lightsail:CreateCertificate",
        "lightsail:CreateContactMethod",
        "lightsail:CreateDistribution",
        "lightsail:CreateDomain",
        "lightsail:CreateDomainEntry",
        "lightsail:DeleteAlarm",
        "lightsail:DeleteCertificate",
        "lightsail:DeleteContactMethod",
        "lightsail:DeleteDistribution",
        "lightsail:DeleteDomain",
        "lightsail:DeleteDomainEntry",
        "lightsail:DetachCertificateFromDistribution",
        "lightsail:Get*",
        "lightsail:IsVpcPeered",
        "lightsail:PutAlarm",
        "lightsail:ResetDistributionCache",
        "lightsail:SendContactMethodVerification",
        "lightsail:SetIpAddressType",
        "lightsail:TagResource",
        "lightsail:TestAlarm",
        "lightsail:UntagResource",
        "lightsail:UpdateDistribution",
        "lightsail:UpdateDistributionBundle",
        "lightsail:UpdateDomainEntry",
        "logs:*",
        "managedblockchain-query:*",
        "managedblockchain:*",
        "mapcredits:*",
        "mobileanalytics:*",
        "networkmanager:*",
        "notifications-contacts:*",
        "notifications:*",
        "organizations:*",
        "payments:*",
        "pricing:*",
        "q:*",
        "quicksight:DescribeAccountSubscription",
        "resource-explorer-2:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "route53:*",
        "route53domains:*",
```

```
        "route53globalresolver:*",
        "s3:CreateMultiRegionAccessPoint",
        "s3:DeleteMultiRegionAccessPoint",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensDashboard",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutMultiRegionAccessPointPolicy",
        "savingsplans:*",
        "servicequotas:*",
        "shield:*",
        "signin:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "sts:*",
        "support:*",
        "supportapp:*",
        "supportplans:*",
        "sustainability:*",
        "tag:GetResources",
        "tax:*",
        "trustedadvisor:*",
        "uxc:*",
        "vendor-insights:ListEntitledSecurityProfiles",
        "waf-regional:*",
        "waf:*",
        "wafv2:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
```

```
      }
    },
    {
      "Sid" : "UsWest2Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "health:*",
        "identitystore-auth:*",
        "identitystore:*",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:ListAliases",
        "networkmanager-chat:*",
        "networkmanager:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "servicequotas:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "support:*",
        "trustedadvisor:*",
        "uxc:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestedRegion" : "us-west-2"
        }
      }
    },
    {
      "Sid" : "RegionFloor",
      "Effect" : "Deny",
      "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestedRegion" : [
            "unspecified",
            "us-east-1",
            "selected-region",
            "us-west-2"
          ]
        }
      }
    }
  ]
}
```

Kebijakan kontrol layanan untuk batas pengeluaran

Jika Anda menggunakan batas pengeluaran, kebijakan kontrol layanan berikut diterapkan ke proyek Anda saat mendekati batas pengeluaran. Untuk informasi selengkapnya tentang batas pengeluaran, lihatBuat batas pengeluaran di AWS Pengaturan.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyBedrockUsage",
    "Effect": "Deny",
    "Action": [
      "bedrock:ApplyGuardrail",
      "bedrock:CallWithBearerToken",
      "bedrock:InvokeAgent",
      "bedrock:InvokeAutomatedReasoningPolicy",
      "bedrock:InvokeDataAutomation",
      "bedrock:InvokeDataAutomationAsync",
      "bedrock:InvokeFlow",
      "bedrock:InvokeInlineAgent",
      "bedrock:InvokeModel",
      "bedrock:InvokeModelWithResponseStream",
      "bedrock:InvokeTool",
      "bedrock:OptimizePrompt",
      "bedrock:Retrieve",
      "bedrock:RetrieveAndGenerate",
      "bedrock:StartFlowExecution",
      "bedrock-mantle:CallWithBearerToken",
      "bedrock-mantle:CreateInference"
    ],
    "Resource": "*"
  }
}
```

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyLambdaUsage",
    "Effect": "Deny",
    "Action": [
      "lambda:DeleteFunctionConcurrency",
      "lambda:InvokeAsync",
      "lambda:InvokeFunction",
      "lambda:InvokeFunctionUrl",
      "lambda:PutFunctionConcurrency"
    ],
    "Resource": "*"
  }
```

```
}
```

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenySageMakerInference",
    "Effect": "Deny",
    "Action": [
      "sagemaker:InvokeEndpoint",
      "sagemaker:InvokeEndpointAsync",
      "sagemaker:InvokeEndpointWithResponseStream"
    ],
    "Resource": "*"
  }
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCompute",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateNatGateway",
        "ec2:CreateVolume",
        "ec2:CreateVpnConnection",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "elasticloadbalancing:CreateLoadBalancer",
        "autoscaling:CreateAutoScalingGroup",
        "ecs:CreateService",
        "eks:CreateCluster",
        "eks:CreateNodegroup",
        "eks:CreateFargateProfile",
        "elasticbeanstalk:CreateEnvironment",
        "apprunner:CreateService",
        "apprunner:ResumeService",
        "batch:CreateComputeEnvironment",
        "elasticmapreduce:RunJobFlow",
        "appstream:CreateFleet"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "DenyLambda",
      "Effect": "Deny",
      "Action": "lambda:CreateFunction",
      "Resource": "*"
    },
    {
      "Sid": "DenyDatabase",
      "Effect": "Deny",
      "Action": [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
        "rds:RestoreDBClusterFromS3",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:RestoreDBInstanceFromS3",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:StartDBCluster",
        "rds:StartDBInstance",
        "dynamodb:CreateTable",
        "dynamodb:CreateGlobalTable",
        "elasticache:CreateCacheCluster",
        "elasticache:CreateReplicationGroup",
        "timestream:CreateDatabase",
        "timestream:CreateTable",
        "memorydb:CreateCluster",
        "es:CreateDomain",
        "aoss:CreateCollection",
        "redshift:CreateCluster",
        "redshift:ResumeCluster",
        "redshift-serverless:CreateWorkgroup",
        "dsql:CreateCluster"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyStorage",
      "Effect": "Deny",
      "Action": [
        "elasticfilesystem:CreateFileSystem",
        "datasync:CreateTask",
        "storagegateway:ActivateGateway",
        "glacier:CreateVault"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySageMaker",
      "Effect": "Deny",
      "Action": [
        "sagemaker:CreateApp",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:StartNotebookInstance"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyBedrock",
      "Effect": "Deny",
      "Action": [
        "bedrock:CreateCustomModelDeployment",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock-mantle:CreateCustomizedModel",
        "bedrock-mantle:CreateFineTuningJob",
        "bedrock-mantle:CreateReservation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyAIML",
      "Effect": "Deny",
      "Action": [
        "kendra:CreateIndex",
        "personalize:CreateSolution",
        "personalize:CreateCampaign",
        "forecast:CreatePredictor",
        "forecast:CreateForecast",
```

```
        "rekognition:CreateProject",
        "lex:CreateBot"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyNetworking",
      "Effect": "Deny",
      "Action": [
        "cloudfront:CreateDistribution",
        "route53:CreateHostedZone",
        "appmesh:CreateMesh"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyApiGatewayCreate",
      "Effect": "Deny",
      "Action": "apigateway:POST",
      "Resource": [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/apis"
      ]
    },
    {
      "Sid": "DenyMessaging",
      "Effect": "Deny",
      "Action": [
        "mq:CreateBroker",
        "kafka:CreateCluster",
        "kafka:CreateVpcConnection",
        "kinesis:CreateStream",
        "firehose:CreateDeliveryStream",
        "kinesisanalytics:CreateApplication",
        "kinesisvideo:CreateStream",
        "sns:CreateTopic",
        "sqs:CreateQueue",
        "events:CreateEventBus",
        "pipes:CreatePipe",
        "scheduler:CreateSchedule"
      ],
      "Resource": "*"
    },
    {
```

```
      "Sid": "DenyAnalytics",
      "Effect": "Deny",
      "Action": [
        "states:CreateStateMachine",
        "glue:CreateJob",
        "glue:CreateCrawler",
        "athena:CreateWorkGroup",
        "appsync:CreateGraphqlApi",
        "appflow:CreateFlow",
        "datazone:CreateDomain",
        "datazone:CreateProject",
        "entityresolution:CreateMatchingWorkflow",
        "datapipeline:CreatePipeline",
        "dataexchange:CreateDataSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyDevTools",
      "Effect": "Deny",
      "Action": [
        "amplify:CreateApp",
        "amplify:CreateBranch",
        "cloud9:CreateEnvironmentEC2",
        "codebuild:CreateProject",
        "codepipeline:CreatePipeline",
        "codedeploy:CreateApplication",
        "cloudformation:CreateStack",
        "cloudformation:CreateStackSet",
        "codeartifact:CreateRepository",
        "codeartifact:CreateDomain"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySecurity",
      "Effect": "Deny",
      "Action": [
        "kms:CreateKey",
        "wafv2:CreateWebACL",
        "cloudhsm:CreateCluster",
        "network-firewall:CreateFirewall",
        "secretsmanager:CreateSecret",
        "acm-pca:CreateCertificateAuthority",
```

```
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
        "ds:CreateDirectory",
        "ds:CreateMicrosoftAD",
        "fms:PutPolicy",
        "payment-cryptography:CreateKey"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyMedia",
      "Effect": "Deny",
      "Action": [
        "medialive:CreateChannel",
        "mediapackage:CreateChannel",
        "mediaconnect:CreateFlow",
        "mediatailor:CreateChannel"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyIoT",
      "Effect": "Deny",
      "Action": [
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iotevents:CreateDetectorModel",
        "iottwinmaker:CreateWorkspace",
        "iotsitewise:CreateAssetModel",
        "iotsitewise:CreatePortal",
        "iotfleetwise:CreateCampaign"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyMisc",
      "Effect": "Deny",
      "Action": [
        "ses:CreateConfigurationSet",
        "ecr:CreateRepository",
        "aps:CreateWorkspace",
        "healthlake:CreateFHIRDatastore",
        "transfer:CreateServer",
        "managedblockchain:CreateNetwork",
```

```
        "managedblockchain:CreateMember",
        "route53-recovery-control-config:CreateCluster",
        "fis:CreateExperimentTemplate",
        "appfabric:CreateAppBundle",
        "appfabric:CreateIngestion",
        "b2bi:CreateProfile",
        "b2bi:CreateTransformer",
        "geo:CreateMap",
        "geo:CreatePlaceIndex",
        "geo:CreateTracker",
        "geo:CreateGeofenceCollection",
        "geo:CreateRouteCalculator"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan kontrol layanan untuk Tingkat Gratis untuk proyek

Kebijakan kontrol layanan berikut mengontrol akses ke AWS layanan yang tersedia di Tingkat Gratis AWS pengalaman baru kami. Kebijakan ini tidak dapat diubah. Untuk mengakses layanan tambahan, tingkatkan akun Anda. Untuk informasi selengkapnya, lihat Tingkatkan akun Anda di AWS Pengaturan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFreeTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",
        "acm:*",
        "aco-automation:*",
        "action-recommendations:*",
        "activate:*",
        "aiops:*",
```

```
        "airflow-serverless:*",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "aoss:*",
        "apigateway:*",
        "app-integrations:*",
        "appconfig:*",
        "appflow:*",
        "application-autoscaling:*",
        "application-signals-mcp:*",
        "application-signals:*",
        "application-transformation:*",
        "applicationinsights:*",
        "appmesh:*",
        "appsync:*",
        "aps:*",
        "arc-zonal-shift:*",
        "artifact:*",
        "athena:*",
        "autoscaling-plans:*",
        "autoscaling:*",
        "aws-external-anthropic:*",
        "aws-marketplace:*",
        "b2bi:*",
        "backup-gateway:*",
        "backup-search:*",
        "backup-storage:*",
        "backup:*",
        "batch:*",
        "bcm-pricing-calculator:*",
        "bedrock-agentcore:*",
        "bedrock-mantle:*",
        "bedrock-websearch:*",
        "bedrock:*",
        "budgets:*",
        "ce:*",
        "chatbot:*",
        "cloud9:*",
        "cloudformation:*",
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*",
        "cloudtrail-data:*",
```

```
        "cloudtrail:*",
        "cloudwatch:*",
        "codeartifact:*",
        "codebuild:*",
        "codecommit:*",
        "codeconnections:*",
        "codedeploy-commands-secure:*",
        "codedeploy:*",
        "codepipeline:*",
        "codestar-connections:*",
        "codestar-notifications:*",
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "compute-optimizer:*",
        "config:*",
        "consoleapp:*",
        "consolidatedbilling:*",
        "cost-optimization-hub:*",
        "customer-verification:*",
        "databrew:*",
        "datapipeline:*",
        "datasync:*",
        "datazone:*",
        "dbqms:*",
        "dlm:*",
        "ds-data:*",
        "ds:*",
        "dsql:*",
        "dynamodb:*",
        "ebs:*",
        "ec2-instance-connect:*",
        "ec2:*",
        "ec2messages:*",
        "ecr-public:*",
        "ecr:*",
        "ecs-mcp:*",
        "ecs:*",
        "eks-auth:*",
        "eks-mcp:*",
        "eks:*",
        "elasticache:*",
        "elasticbeanstalk:*",
        "elasticfilesystem:*",
```

```
        "elasticloadbalancing:*",
        "entityresolution:*",
        "es:*",
        "events:*",
        "evidently:*",
        "execute-api:*",
        "finops-agent:*",
        "freertos:*",
        "freetier:*",
        "geo-maps:*",
        "geo-places:*",
        "geo-routes:*",
        "geo:*",
        "glue:*",
        "groundtruthlabeling:*",
        "health:*",
        "iam:*",
        "identitystore-auth:*",
        "identitystore:*",
        "imagebuilder:*",
        "internetmonitor:*",
        "invoicing:*",
        "iot-device-tester:*",
        "iot:*",
        "iotdeviceadvisor:*",
        "iotfleethub:*",
        "iotjobsdata:*",
        "iotmanagedintegrations:*",
        "iotsitewise:*",
        "iottwinmaker:*",
        "iotwireless:*",
        "kms:*",
        "lakeformation:*",
        "lambda:*",
        "launchwizard:*",
        "lex:*",
        "license-manager-linux-subscriptions:*",
        "license-manager-user-subscriptions:*",
        "license-manager:*",
        "logs:*",
        "mgn:*",
        "migrationhub-orchestrator:*",
        "migrationhub-strategy:*",
        "mpa:*",
```

```
        "mq:*",
        "networkflowmonitor:*",
        "networkmanager-chat:*",
        "networkmanager:*",
        "networkmonitor:*",
        "notifications-contacts:*",
        "notifications:*",
        "nova-act:*",
        "oam:*",
        "observabilityadmin:*",
        "opensearch:*",
        "organizations:*",
        "osis:*",
        "payment-cryptography:*",
        "pi:*",
        "pipes:*",
        "polly:*",
        "pricing:*",
        "q:DeleteConversation",
        "q:GenerateCodeFromCommands",
        "q:GenerateCodeRecommendations",
        "q:GetConversation",
        "q:GetIdentityMetadata",
        "q:GetTroubleshootingResults",
        "q:ListConversations",
        "q:PassRequest",
        "q:SendEvent",
        "q:SendMessage",
        "q:StartConversation",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateConversation",
        "q:UpdateTroubleshootingCommandResult",
        "q:UsePlugin",
        "ram:*",
        "rbin:*",
        "rds-data:*",
        "rds-db:*",
        "rds:*",
        "rekognition:*",
        "resource-explorer-2:*",
        "resource-explorer:*",
        "resource-groups:*",
        "rhelkb:*",
```

```
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "route53:*",
        "route53domains:*",
        "route53globalresolver:*",
        "route53profiles:*",
        "route53resolver:*",
        "rum:*",
        "s3-object-lambda:*",
        "s3:*",
        "s3express:*",
        "s3files:*",
        "s3tables:*",
        "s3vectors:*",
        "sagemaker-data-science-assistant:*",
        "sagemaker-geospatial:*",
        "sagemaker-mlflow:*",
        "sagemaker-unified-studio-mcp:*",
        "sagemaker:*",
        "scheduler:*",
        "schemas:*",
        "secretsmanager:*",
        "serverlessrepo:*",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicediscovery:*",
        "serviceextract:*",
        "servicequotas:*",
        "ses:*",
        "signer:*",
        "signin:*",
        "sns:*",
        "sqlworkbench:*",
        "sqs:*",
        "ssm-contacts:*",
        "ssm-guiconnect:*",
        "ssm-incidents:*",
```

```
        "ssm-quicksetup:*",
        "ssm-sap:*",
        "ssm:*",
        "ssmmessages:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "states:*",
        "sts:*",
        "support:*",
        "swf:*",
        "synthetics:*",
        "tag:*",
        "tax:*",
        "timestream-influxdb:*",
        "ts:*",
        "uxc:*",
        "verifiedpermissions:*",
        "vpce:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*",
        "xray:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2CapacityBlock",
      "Effect": "Deny",
      "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
      "Resource": "*"
    },
    {
      "Sid": "DenyRestrictedAgreements",
      "Effect": "Deny",
      "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
      "Resource": [
        "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm",
        "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact:::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact:::agreement/agreement-HZTdNwJuqOKLReXC"
      ]
    },
```

```
    {
      "Sid": "DenyDocDB",
      "Effect": "Deny",
      "Action": ["rds:CreateDBCluster", "rds:CreateDBInstance"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:DatabaseEngine": ["docdb"]
        }
      }
    },
    {
      "Sid": "DenyCloudWAN",
      "Effect": "Deny",
      "Action": [
        "networkmanager:CreateCoreNetwork",
        "networkmanager:CreateConnectAttachment",
        "networkmanager:CreateConnectPeer",
        "networkmanager:CreateVpcAttachment",
        "networkmanager:CreateSiteToSiteVpnAttachment",
        "networkmanager:CreateTransitGatewayPeering",
        "networkmanager:CreateDirectConnectGatewayAttachment",
        "networkmanager:PutCoreNetworkPolicy",
        "networkmanager:ExecuteCoreNetworkChangeSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyTransitGatewayAndVPN",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayConnect",
        "ec2:CreateTransitGatewayConnectPeer",
        "ec2:CreateTransitGatewayMulticastDomain",
        "ec2:CreateTransitGatewayPeeringAttachment",
        "ec2:CreateTransitGatewayPolicyTable",
        "ec2:CreateTransitGatewayPrefixListReference",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:CreateClientVpnEndpoint",
        "ec2:CreateClientVpnRoute",
```

```
        "ec2:AuthorizeClientVpnIngress",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:CreateCustomerGateway"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySageMakerGroundTruth",
      "Effect": "Deny",
      "Action": [
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateWorkteam",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateHumanTaskUi"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyGlacierStorageClasses",
      "Effect": "Deny",
      "Action": ["s3:PutObject"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-storage-class": ["DEEP_ARCHIVE", "GLACIER"]
        }
      }
    },
    {
      "Sid": "DenyEC2Fleet",
      "Effect": "Deny",
      "Action": ["ec2:CreateFleet"],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2BYOLAndLicenseConfigurations",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances", "ec2:StartInstances"],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals": {
```

```
          "ec2:Tenancy": "host"
        }
      }
    },
    {
      "Sid": "DenyEC2InstanceStoreRootDevice",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances"],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:RootDeviceType": "instance-store"
        }
      }
    },
    {
      "Sid": "DenyLicenseManagerAssociation",
      "Effect": "Deny",
      "Action": ["license-manager:CreateLicenseConfiguration"],
      "Resource": "*"
    },
    {
      "Sid": "DenyIAMRestrictedActions",
      "Effect": "Deny",
      "Action": [
        "iam:*Alias*",
        "iam:*Organizations*",
        "iam:*Provider*",
        "iam:SetSecurityTokenServicePreferences",
        "iam:*LoginProfile*",
        "iam:CreateGroup",
        "iam:AttachGroupPolicy",
        "iam:AddUserToGroup",
        "iam:PutGroupPolicy",
        "iam:UpdateGroup",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "iam:UploadServerCertificate",
        "iam:UploadSigningCertificate",
        "iam:TagServerCertificate",
        "iam:UntagServerCertificate"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "DenySSOCreateInstance",
      "Effect": "Deny",
      "Action": ["sso:CreateInstance"],
      "Resource": "*"
    },
    {
      "Sid": "DenyRequestSpotInstances",
      "Effect": "Deny",
      "Action": ["ec2:RequestSpotInstances"],
      "Resource": "*"
    },
    {
      "Sid": "DenySpotMarketType",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:InstanceMarketType": "spot"
        }
      }
    },
    {
      "Sid": "DenyReservedInstanceAndCapacityPurchases",
      "Effect": "Deny",
      "Action": [
        "athena:CreateCapacityReservation",
        "cloudfront:CreateSavingsPlan",
        "dynamodb:PurchaseReservedCapacityOfferings",
        "ec2:AllocateHosts",
        "ec2:CreateCapacityReservation",
        "ec2:CreateCapacityReservationBySplitting",
        "ec2:CreateCapacityReservationCancellationQuote",
        "ec2:CreateCapacityReservationFleet",
        "ec2:PurchaseHostReservation",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:PurchaseScheduledInstances",
        "elasticache:PurchaseReservedCacheNodesOffering",
        "es:PurchaseReservedElasticsearchInstanceOffering",
        "es:PurchaseReservedInstanceOffering",
        "glacier:PurchaseProvisionedCapacity",
        "memorydb:PurchaseReservedNodesOffering",
        "rds:PurchaseReservedDBInstancesOffering",
```

```
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering",
        "sagemaker:CreateReservedCapacity",
        "savingsplans:CreateSavingsPlan"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyExportableCertificateRequests",
      "Effect": "Deny",
      "Action": ["acm:RequestCertificate"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "acm:AllowExport": "true"
        }
      }
    }
  ]
}
```

Kebijakan kontrol layanan untuk Paket Berbayar untuk proyek

Kebijakan kontrol layanan berikut mengontrol akses ke AWS layanan yang tersedia dalam Paket Berbayar AWS pengalaman baru kami. Kebijakan ini tidak dapat diubah. Untuk mengakses layanan tambahan, aktifkan fitur-fitur canggih. Untuk informasi selengkapnya, lihat Aktifkan lanjutan AWS fitur.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPaidTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",
        "acm:*",
        "aco-automation:*",
        "action-recommendations:*",
```

```
        "activate:*",
        "aidevops:*",
        "aiops:*",
        "airflow-serverless:*",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "aoss:*",
        "apigateway:*",
        "app-integrations:*",
        "appconfig:*",
        "appfabric:*",
        "appflow:*",
        "application-autoscaling:*",
        "application-signals-mcp:*",
        "application-signals:*",
        "application-transformation:*",
        "applicationinsights:*",
        "appmesh:*",
        "appsync:*",
        "aps:*",
        "arc-zonal-shift:*",
        "artifact:*",
        "athena:*",
        "autoscaling-plans:*",
        "autoscaling:*",
        "aws-external-anthropic:*",
        "aws-marketplace:*",
        "b2bi:*",
        "backup-gateway:*",
        "backup-search:*",
        "backup-storage:*",
        "backup:*",
        "batch:*",
        "bcm-pricing-calculator:*",
        "bedrock-agentcore:*",
        "bedrock-mantle:*",
        "bedrock-websearch:*",
        "bedrock:*",
        "budgets:*",
        "ce:*",
        "chatbot:*",
        "cloud9:*",
        "cloudformation:*",
```

```
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*",
        "cloudtrail-data:*",
        "cloudtrail:*",
        "cloudwatch:*",
        "codeartifact:*",
        "codebuild:*",
        "codecommit:*",
        "codeconnections:*",
        "codedeploy-commands-secure:*",
        "codedeploy:*",
        "codeguru-profiler:*",
        "codeguru-reviewer:*",
        "codeguru-security:*",
        "codepipeline:*",
        "codestar-connections:*",
        "codestar-notifications:*",
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "compute-optimizer:*",
        "config:*",
        "consoleapp:*",
        "consolidatedbilling:*",
        "cost-optimization-hub:*",
        "customer-verification:*",
        "databrew:*",
        "dataexchange:*",
        "datapipeline:*",
        "datasync:*",
        "datazone:*",
        "dbqms:*",
        "devops-guru:*",
        "dlm:*",
        "docdb-elastic:*",
        "ds-data:*",
        "ds:*",
        "dsql:*",
        "dynamodb:*",
        "ebs:*",
        "ec2-instance-connect:*",
        "ec2:*",
        "ec2messages:*",
```

```
        "ecr-public:*",
        "ecr:*",
        "ecs-mcp:*",
        "ecs:*",
        "eks-auth:*",
        "eks-mcp:*",
        "eks:*",
        "elasticache:*",
        "elasticbeanstalk:*",
        "elasticfilesystem:*",
        "elasticloadbalancing:*",
        "elasticmapreduce:*",
        "emr-containers:*",
        "emr-serverless:*",
        "entityresolution:*",
        "es:*",
        "events:*",
        "evidently:*",
        "execute-api:*",
        "finops-agent:*",
        "firehose:*",
        "fis:*",
        "fms:*",
        "forecast:*",
        "freertos:*",
        "freetier:*",
        "geo-maps:*",
        "geo-places:*",
        "geo-routes:*",
        "geo:*",
        "glacier:*",
        "glue:*",
        "groundtruthlabeling:*",
        "health:*",
        "iam:*",
        "identitystore-auth:*",
        "identitystore:*",
        "imagebuilder:*",
        "internetmonitor:*",
        "invoicing:*",
        "iot-device-tester:*",
        "iot:*",
        "iotdeviceadvisor:*",
        "iotfleethub:*",
```

```
        "iotjobsdata:*",
        "iotmanagedintegrations:*",
        "iotsitewise:*",
        "iottwinmaker:*",
        "iotwireless:*",
        "kafka-cluster:*",
        "kafka:*",
        "kafkaconnect:*",
        "kinesis:*",
        "kinesisanalytics:*",
        "kinesisvideo:*",
        "kms:*",
        "lakeformation:*",
        "lambda:*",
        "launchwizard:*",
        "lex:*",
        "license-manager-linux-subscriptions:*",
        "license-manager-user-subscriptions:*",
        "license-manager:*",
        "logs:*",
        "managedblockchain-query:*",
        "managedblockchain:*",
        "mapcredits:*",
        "memorydb:*",
        "mgn:*",
        "migrationhub-orchestrator:*",
        "migrationhub-strategy:*",
        "mpa:*",
        "mq:*",
        "neptune-db:*",
        "neptune-graph:*",
        "network-firewall:*",
        "networkflowmonitor:*",
        "networkmanager-chat:*",
        "networkmanager:*",
        "networkmonitor:*",
        "notifications-contacts:*",
        "notifications:*",
        "nova-act:*",
        "oam:*",
        "observabilityadmin:*",
        "opensearch:*",
        "organizations:*",
        "osis:*",
```

```
        "payment-cryptography:*",
        "personalize:*",
        "pi:*",
        "pipes:*",
        "polly:*",
        "pricing:*",
        "q:DeleteConversation",
        "q:GenerateCodeFromCommands",
        "q:GenerateCodeRecommendations",
        "q:GetConversation",
        "q:GetIdentityMetadata",
        "q:GetTroubleshootingResults",
        "q:ListConversations",
        "q:PassRequest",
        "q:SendEvent",
        "q:SendMessage",
        "q:StartConversation",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateConversation",
        "q:UpdateTroubleshootingCommandResult",
        "q:UsePlugin",
        "ram:*",
        "rbin:*",
        "rds-data:*",
        "rds-db:*",
        "rds:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "rekognition:*",
        "resource-explorer-2:*",
        "resource-explorer:*",
        "resource-groups:*",
        "rhelkb:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "route53:*",
        "route53domains:*",
        "route53globalresolver:*",
        "route53profiles:*",
        "route53resolver:*",
        "rum:*",
```

```
        "s3-object-lambda:*",
        "s3:*",
        "s3express:*",
        "s3files:*",
        "s3tables:*",
        "s3vectors:*",
        "sagemaker-data-science-assistant:*",
        "sagemaker-geospatial:*",
        "sagemaker-mlflow:*",
        "sagemaker-unified-studio-mcp:*",
        "sagemaker:*",
        "scheduler:*",
        "schemas:*",
        "secretsmanager:*",
        "securityagent:*",
        "serverlessrepo:*",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicediscovery:*",
        "serviceextract:*",
        "servicequotas:*",
        "ses:*",
        "signer:*",
        "signin:*",
        "sms-voice:*",
        "sns:*",
        "social-messaging:*",
        "sqlworkbench:*",
        "sqs:*",
        "ssm-contacts:*",
        "ssm-guiconnect:*",
        "ssm-incidents:*",
        "ssm-quicksetup:*",
        "ssm-sap:*",
        "ssm:*",
        "ssmmessages:*",
        "sso-directory:*",
        "sso-oauth:*",
```

```
        "sso:*",
        "states:*",
        "storagegateway:*",
        "sts:*",
        "support:*",
        "swf:*",
        "synthetics:*",
        "tag:*",
        "tax:*",
        "textract:*",
        "timestream-influxdb:*",
        "timestream:*",
        "transcribe:*",
        "translate:*",
        "ts:*",
        "uxc:*",
        "verifiedpermissions:*",
        "vpce:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*",
        "xray:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2CapacityBlock",
      "Effect": "Deny",
      "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
      "Resource": "*"
    },
    {
      "Sid": "DenyRestrictedAgreements",
      "Effect": "Deny",
      "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
      "Resource": [
        "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm",
        "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact:::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact:::agreement/agreement-HZTdNwJuqOKLReXC"
      ]
    },
    {
```

```
      "Sid": "DenyCloudWAN",
      "Effect": "Deny",
      "Action": [
        "networkmanager:CreateCoreNetwork",
        "networkmanager:CreateConnectAttachment",
        "networkmanager:CreateConnectPeer",
        "networkmanager:CreateVpcAttachment",
        "networkmanager:CreateSiteToSiteVpnAttachment",
        "networkmanager:CreateTransitGatewayPeering",
        "networkmanager:CreateDirectConnectGatewayAttachment",
        "networkmanager:PutCoreNetworkPolicy",
        "networkmanager:ExecuteCoreNetworkChangeSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyTransitGatewayAndVPN",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayConnect",
        "ec2:CreateTransitGatewayConnectPeer",
        "ec2:CreateTransitGatewayMulticastDomain",
        "ec2:CreateTransitGatewayPeeringAttachment",
        "ec2:CreateTransitGatewayPolicyTable",
        "ec2:CreateTransitGatewayPrefixListReference",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:CreateClientVpnEndpoint",
        "ec2:CreateClientVpnRoute",
        "ec2:AuthorizeClientVpnIngress",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:CreateCustomerGateway"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySageMakerGroundTruth",
      "Effect": "Deny",
```

```
      "Action": [
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateWorkteam",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateHumanTaskUi"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2Fleet",
      "Effect": "Deny",
      "Action": ["ec2:CreateFleet"],
      "Resource": "*"
    },
    {
      "Sid": "DenyEC2BYOLAndLicenseConfigurations",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances", "ec2:StartInstances"],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:Tenancy": "host"
        }
      }
    },
    {
      "Sid": "DenyEC2InstanceStoreRootDevice",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances"],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:RootDeviceType": "instance-store"
        }
      }
    },
    {
      "Sid": "DenyLicenseManagerAssociation",
      "Effect": "Deny",
      "Action": ["license-manager:CreateLicenseConfiguration"],
      "Resource": "*"
    },
    {
      "Sid": "DenyIAMRestrictedActions",
```

```
      "Effect": "Deny",
      "Action": [
        "iam:*Alias*",
        "iam:*Organizations*",
        "iam:*Provider*",
        "iam:SetSecurityTokenServicePreferences",
        "iam:*LoginProfile*",
        "iam:CreateGroup",
        "iam:AttachGroupPolicy",
        "iam:AddUserToGroup",
        "iam:PutGroupPolicy",
        "iam:UpdateGroup",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "iam:UploadServerCertificate",
        "iam:UploadSigningCertificate",
        "iam:TagServerCertificate",
        "iam:UntagServerCertificate"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenySSOCreateInstance",
      "Effect": "Deny",
      "Action": ["sso:CreateInstance"],
      "Resource": "*"
    },
    {
      "Sid": "DenyRequestSpotInstances",
      "Effect": "Deny",
      "Action": ["ec2:RequestSpotInstances"],
      "Resource": "*"
    },
    {
      "Sid": "DenySpotMarketType",
      "Effect": "Deny",
      "Action": ["ec2:RunInstances"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:InstanceMarketType": "spot"
        }
      }
    },
```

```
    {
      "Sid": "DenyReservedInstanceAndCapacityPurchases",
      "Effect": "Deny",
      "Action": [
        "athena:CreateCapacityReservation",
        "cloudfront:CreateSavingsPlan",
        "dynamodb:PurchaseReservedCapacityOfferings",
        "ec2:AllocateHosts",
        "ec2:CreateCapacityReservation",
        "ec2:CreateCapacityReservationBySplitting",
        "ec2:CreateCapacityReservationCancellationQuote",
        "ec2:CreateCapacityReservationFleet",
        "ec2:PurchaseHostReservation",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:PurchaseScheduledInstances",
        "elasticache:PurchaseReservedCacheNodesOffering",
        "es:PurchaseReservedElasticsearchInstanceOffering",
        "es:PurchaseReservedInstanceOffering",
        "glacier:PurchaseProvisionedCapacity",
        "memorydb:PurchaseReservedNodesOffering",
        "rds:PurchaseReservedDBInstancesOffering",
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering",
        "sagemaker:CreateReservedCapacity",
        "savingsplans:CreateSavingsPlan"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyExportableCertificateRequests",
      "Effect": "Deny",
      "Action": ["acm:RequestCertificate"],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "acm:AllowExport": "true"
        }
      }
    }
  ]
}
```

Kebijakan pengendalian sumber daya untuk proyek

Berikut ini adalah kebijakan pengendalian sumber daya untuk sumber daya dalam proyek. Kebijakan ini tidak dapat diubah:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAnyoneOutsideMyOrgAndAWS",
      "Effect" : "Deny",
      "Principal" : "*",
      "Action" : [
        "aoss:*",
        "appconfig:*",
        "appstream:*",
        "autoscaling:*",
        "codebuild:*",
        "codecommit:*",
        "cognito-identity:*",
        "cognito-idp:*",
        "comprehend:*",
        "comprehendmedical:*",
        "dax:*",
        "dynamodb:*",
        "ecr:*",
        "health:*",
        "kinesisvideo:*",
        "kms:*",
        "logs:*",
        "s3:*",
        "secretsmanager:*",
        "sqs:*",
        "sts:*",
        "support:*",
        "textract:*",
        "transcribe:*",
        "translate:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "BoolIfExists" : {
          "aws:PrincipalIsAWSService" : "false"
```

```
        },
        "Null" : {
          "aws:PrincipalARN" : "false"
        },
        "StringNotEqualsIfExists" : {
          "aws:PrincipalOrgID" : "${aws:ResourceOrgID}"
        }
      }
    },
    {
      "Sid" : "DenyAWSWhenItsNotMyOrgsSourceAccount",
      "Effect" : "Deny",
      "Principal" : "*",
      "Action" : [
        "aoss:*",
        "appconfig:*",
        "appstream:*",
        "autoscaling:*",
        "codebuild:*",
        "codecommit:*",
        "cognito-identity:*",
        "cognito-idp:*",
        "comprehend:*",
        "comprehendmedical:*",
        "dax:*",
        "dynamodb:*",
        "ecr:*",
        "health:*",
        "kinesisvideo:*",
        "kms:*",
        "logs:*",
        "s3:*",
        "secretsmanager:*",
        "sqs:*",
        "sts:*",
        "support:*",
        "textract:*",
        "transcribe:*",
        "translate:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:SourceAccount" : "false"
```

```
        },
        "StringNotEquals" : {
          "aws:SourceOrgID" : "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

Beralih antar proyek

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda hanya dapat mengelola AWS sumber daya untuk satu proyek pada satu waktu. Anda selalu dapat mengetahui proyek mana Anda berada berdasarkan nama di kanan atas AWS konsol.

Beralih antar proyek untuk sesi aktif dari Konsol Manajemen AWS

Untuk beralih antar proyek untuk sesi aktif dari Konsol Manajemen AWS

1. Buka Konsol Manajemen AWS.
2. Pilih nama proyek Anda di kanan atas Konsol Manajemen AWS.
3. Pilih Beralih proyek.
4. Di bawah Sesi aktif, pilih sesi aktif. Sesi aktif adalah sesi yang telah masuk hingga 12 jam. Waktu sesi aktif tidak dapat diubah.
5. Anda akan diarahkan ke halaman AWS beranda konsol untuk proyek baru Anda.

Beralih antar proyek di AWS Pengaturan

Untuk beralih antar proyek di AWS Pengaturan

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih proyek yang ingin Anda akses.

3. Di bilah navigasi di kanan atas, pilih Buat dan kelola infrastruktur cloud.

   Anda akan diarahkan kembali ke Konsol Manajemen AWS proyek baru Anda.

Beralih antar proyek dari Konsol Manajemen AWS

Untuk beralih antar proyek dari Konsol Manajemen AWS

1. Buka Konsol Manajemen AWS.
2. Pilih Kelola proyek.
3. Di AWS Pengaturan, pilih proyek yang ingin Anda akses.
4. Di bilah navigasi di kanan atas, pilih Buat dan kelola infrastruktur cloud.

   Anda akan diarahkan kembali ke Konsol Manajemen AWS proyek baru Anda.

Undang anggota tim untuk berkolaborasi AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat memberikan anggota tim akses ke proyek Anda. Saat Anda berbagi proyek dengan anggota tim, Anda tidak dapat mengontrol AWS layanan mana yang dapat mereka akses. Baik Anda dan anggota tim memiliki akses admin ke proyek. Ini berarti, anggota tim memiliki izin untuk mengakses semua AWS layanan yang tersedia untuk proyek Anda. Ini termasuk membuat kontrol akses untuk layanan dan aplikasi. Namun, mereka tidak memiliki izin untuk melakukan tindakan administratif atau keuangan, seperti menghapus proyek Anda atau mengubah batas pengeluaran. Untuk melihat anggota tim mana yang telah memodi AWS fikasi layanan, lihatPantau proyek Anda menggunakan AWS CloudTrail.

Di AWS Pengaturan, Anda dan anggota tim Anda memiliki tingkat akses yang berbeda. Untuk melihat kebijakan AWS terkelola yang diterapkan pada anggota tim, lihat AWSManagedSettingsReadOnlyAccess. Untuk melihat kebijakan AWS terkelola yang diterapkan pada pemilik proyek, lihat AWSManagedSettingsAdminAccess.

Pertimbangkan hal berikut saat menambahkan anggota tim ke proyek Anda.

Pertimbangan untuk anggota tim

Anggota tim dapat melakukan tindakan berikut:

- Melihat, membuat, mengedit, menghapus, dan memodifikasi AWS sumber daya dalam proyek.
- Peng AWS aturan Akses.
- Lihat batas pengeluaran.
- Minta kenaikan kuota untuk suatu AWS layanan.

Anggota tim tidak dapat melakukan tindakan berikut:

- Tinggalkan proyek.
- Lakukan tindakan root apa pun. Untuk informasi selengkapnya, lihat AWS tindakan untuk pemilik proyek.
- Undang anggota tim untuk proyek.
- Kelola izin anggota tim mana pun.
- Hapus setiap anggota tim dari proyek.
- Mengubah nama proyek.
- Menyiapkan atau memperbarui metode pembayaran.
- Lihat atau perbarui detail penagihan, termasuk alamat atau nomor telepon.
- Lihat atau perbarui informasi pajak.
- Tingkatkan dari Tingkat Gratis ke Paket Berbayar.
- Tetapkan atau ubah batas pengeluaran per proyek.
- Lihat tren biaya untuk setiap proyek.
- Lihat total AWS pengeluaran di semua proyek.
- Lihat dan tukarkan kredit promosi Tingkat Non-Gratis.
- Lihat sisa kredit dan tanggal kedaluwarsa untuk semua jenis kredit.
- Lihat riwayat kredit lengkap termasuk kredit yang diperoleh, diterapkan, dan kedaluwarsa.
- Lihat bagaimana kredit diterapkan di seluruh proyek.
- Lihat saldo yang belum dibayar.
- Jalankan pembayaran ke AWS.

- Unduh faktur atau lihat transaksi sebelumnya.
- Memvalidasi bahwa AWS biaya sudah benar, termasuk kredit yang diterapkan.
- Terima komunikasi penagihan tingkat akun manajemen.
- Dapatkan bantuan untuk masalah penagihan di tingkat organisasi.
- Minta kenaikan kuota untuk kuota akun dan tagihan.

Bagaimana anggota tim mengakses AWS sumber daya

Peng AWS alaman baru kami menciptakan peran terkait layanan untuk organisasi yang berisi semua proyek Anda yang tidak dapat Anda modifikasi. Peran ini secara berkala memverifikasi bahwa catatan internal anggota tim Anda tetap sinkron dengan anggota tim Anda yang sebenarnya.

Peran tertaut layanan AWSServiceRoleForAccountAccessManager memercayai layanan berikut untuk mengambil peran tersebut:

- `account-access.amazonaws.com`

Kebijakan izin peran yang dinam `AccountAccessManagerServiceRolePolicy` ai memungkinkan pengelola akses akun menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan:`organizations:ListAccounts`,`organizations:ListAWSServiceAccessForOrganiza` `organizations:DescribeAccount` pada `"arn:aws:organizations::*:account/o-*/*"`

Untuk informasi selengkapnya, lihat AWS Manajer Akses Akun.

Undang anggota tim untuk berkolaborasi AWS Pengaturan

Untuk mengundang anggota tim, Anda mengirimkan undangan kepada mereka dari halaman Tim di Peng AWS aturan. Anggota tim memiliki waktu 14 hari untuk menerima undangan mereka. Anggota tim harus membuat ID AWS Builder untuk mengakses proyek Anda. Mereka dapat melakukan ini menggunakan Daftar untuk AWS (baru).

Undang anggota tim untuk berkolaborasi AWS Pengaturan

1. Buka AWS Pengaturan di https://settings.aws.com.

2. Di panel navigasi utama, pilih Tim.
3. Pilih Undang anggota tim baru.
4. Untuk Email, masukkan alamat email atau daftar alamat email. Pisahkan alamat email dengan koma (,) atau titik koma (;).
5. Pilih satu atau lebih proyek untuk dibagikan dengan anggota tim baru Anda.
6. Pilih Kirim undangan.

Jika anggota tim Anda tidak mendapatkan undangan, minta mereka untuk memeriksa folder spam dan sampah mereka.

Undang anggota tim ke proyek di AWS Pengaturan

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat mengundang anggota tim untuk mengakses proyek. Untuk informasi tentang apa yang dapat dilakukan anggota tim dalam sebuah proyek, lihatUndang anggota tim untuk berkolaborasi AWS Pengaturan.

Untuk mengundang anggota tim ke sebuah proyek

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih proyek yang ingin Anda akses.
3. Untuk Anggota, pilih Undang anggota tim baru.
4. Untuk Email, masukkan alamat email atau daftar alamat email. Pisahkan alamat email dengan koma (,) atau titik koma (;).
5. Pilih proyek untuk dibagikan dengan anggota tim baru Anda.
6. Pilih Kirim undangan.

Jika anggota tim Anda tidak mendapatkan undangan, minta mereka untuk memeriksa folder spam dan sampah mereka.

Menghapus anggota tim dari proyek di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat menghapus anggota tim dari proyek kapan saja. Anggota tim Anda tidak dapat melakukan ini sendiri. Ketika Anda menghapus anggota tim, mereka tidak akan lagi memiliki akses ke proyek itu. Sumber daya apa pun yang dibuat anggota tim Anda tetap ada di proyek Anda dan Anda harus mengelolanya.

Untuk menghapus anggota tim dari proyek

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih proyek yang ingin Anda akses.
3. Di tab Anggota, pilih anggota yang ingin Anda hapus dari proyek, lalu pilih Hapus.
4. Konfirmasikan pilihan Anda dan pilih Hapus.

Anggota tim masih menjadi bagian dari tim Anda dan Anda dapat menambahkannya ke proyek lain. Untuk menghapus anggota tim sepenuhnya dari Peng AWS aturan, lihatMenghapus anggota tim di AWS Pengaturan.

Menghapus anggota tim di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat menggunakan halaman Tim untuk menghapus anggota tim dari semua proyek. Mereka secara otomatis akan kehilangan akses ke proyek apa pun. Sumber daya apa pun yang dibuat anggota tim tidak akan dihapus.

Untuk menghapus anggota tim

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Tim.
3. Pilih kotak centang untuk anggota tim yang ingin Anda hapus.
4. Pilih Hapus.
5. Konfirmasikan pilihan Anda dan pilih Hapus.

Mencabut undangan ke anggota tim di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat mencabut undangan yang tertunda. Undangan akan tetap berada di AWS Pengaturan selama 14 hari. Saat Anda mencabut undangan yang tertunda, tautan akses di email undangan akan dinonaktifkan. Anda tidak dapat mencabut undangan yang diterima, melainkan menghapus anggota tim. Untuk informasi selengkapnya, lihat Menghapus anggota tim di AWS Pengaturan.

Untuk mencabut undangan

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Tim.
3. Pilih kotak centang untuk anggota tim yang memiliki undangan tertunda.
4. Pilih Cabut.
5. Konfirmasikan pilihan Anda dan pilih Cabut undangan.

Mengirim ulang undangan ke anggota tim di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat mengirim ulang undangan anggota tim untuk undangan yang dicabut, kedaluwarsa, atau ditolak. Saat Anda mengirim ulang undangan, anggota tim Anda menerima email baru dengan tanggal kedaluwarsa 14 hari sejak Anda mengirim ulang undangan.

Mengirim ulang undangan

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Tim.
3. Pilih kotak centang untuk anggota tim yang memiliki undangan yang dicabut, kedaluwarsa, atau ditolak.
4. Pilih K irim Ulang.
5. Konfirmasikan pilihan Anda dan pilih Kirim Ulang Und angan.

Tingkatkan akun Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Saat Anda mendaftar dengan Daftar untuk AWS (baru), akun Anda berada di Tingkat Gratis. Di Tingkat Gratis, Anda menerima kredit pendaftaran USD $100 dan mendapatkan kredit tambahan hingga $100. Ketika Anda kehabisan kredit atau memiliki akun yang lebih dari 6 bulan, Anda harus meningkatkan ke Paket Berbayar. Anda juga dapat meningkatkan ke Paket Berbayar kapan saja. Saat Anda meningkatkan ke Paket Berbayar, Anda memiliki akses ke layanan yang tercantum diLayanan AWS termasuk dalam Paket Berbayar baru kami AWS pengalaman.

Pertimbangan untuk meningkatkan akun Anda

Pertimbangkan hal berikut saat Anda meningkatkan ke Paket Berbayar:

- Anda tidak dapat meningkatkan proyek individual. Semua proyek Anda ditingkatkan saat Anda meningkatkan akun Anda.
- Saat Anda meningkatkan, Anda akan memiliki akses ke layanan Selalu Gratis dan penawaran uji coba jangka pendek.

- Anda memenuhi syarat untuk kredit promosi dan diskon lainnya.
- Anda harus membayar biaya yang melebihi saldo kredit.
- Anda dapat membuat batas pengeluaran untuk menetapkan maksimum yang akan Anda bayar per bulan untuk sebuah proyek. Untuk informasi selengkapnya, lihat Buat batas pengeluaran di AWS Pengaturan.
- Anda tidak dapat menunjuk proyek apa pun yang sesuai dengan HIPAA atau SEC.
- Akun Anda tidak ditutup saat kredit habis.
- Ini tidak meningkatkan Anda keDaftar untuk AWS (lanjutan). Tak satu pun fitur yang hanya didukung untuk akun yang dibuat menggunakan Daftar untuk AWS (lanjutan) akan tersedia saat Anda meningkatkan akun Anda. Namun, Anda bisa Aktifkan lanjutan AWS fitur untuk akun Anda.
- Anda tidak dapat membalikkan proses peningkatan.

Tingkatkan akun Anda di AWS Pengaturan

Untuk meng-upgrade akun Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Pilih Tingkatkan.
4. Pilih Mulai.
5. Tambahkan metode pembayaran Anda.

   Berdasarkan lokasi Anda, Anda mungkin perlu memberikan beberapa informasi pajak.
6. Pilih Upgrade akun.
7. Pilih Lanjutkan untuk kembali ke bangunan atau pilih Tet apkan batas pengelu aran untuk menetapkan batas pengeluaran. Untuk informasi lebih lanjut tentang batas pengeluaran, lihatBuat batas pengeluaran di AWS Pengaturan.
8. Pilih Pergi ke konsol.

Upgrade Anda selesai.

Buat batas pengeluaran di AWS Pengaturan

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Apa itu batas pengeluaran?

Batas pengeluaran memungkinkan pengembang untuk menggunakan AWS dengan keyakinan bahwa mereka dapat beroperasi dalam anggaran yang dapat diprediksi dan terkendali. Gunakan batas pengeluaran untuk menetapkan jumlah paling banyak yang akan Anda bayar per bulan untuk sebuah proyek. Batas pengeluaran berada di tingkat proyek. Anda dapat memiliki batas pengeluaran pada beberapa proyek Anda dan memiliki proyek lain tanpa batas pengeluaran.

Jika penggunaan Anda dalam proyek mencapai batasnya, AWS jeda proyek yang menghentikan sumber dayanya sehingga biaya Anda tetap di dalamnya. Batas pengeluaran dirancang untuk beban kerja eksperimen, pembelajaran, dan kotak pasir. Mereka dapat digunakan untuk lingkungan produksi ketika dapat diterima untuk memiliki jeda singkat sumber daya Anda jika aplikasi Anda mengeluarkan biaya yang tidak terduga.

Batas pengeluaran dapat dilihat oleh siapa saja yang memiliki akses proyek, tetapi hanya dapat dikelola oleh pemilik proyek. Anda harus menggunakan Paket Berbayar untuk membuat batas pengeluaran. Untuk informasi selengkapnya, lihat Tingkatkan akun Anda di AWS Pengaturan.

Batas pengeluaran adalah jenis AWS Anggaran.

Tetapkan batas pengeluaran Anda

Batas pengeluaran Anda adalah batas biaya sebelum pajak proyek Anda, bukan biaya. Ketika Anda menetapkan batas pengeluaran, nilai minimum yang diizinkan adalah lebih besar dari $20 atau perkiraan konservatif dari kemungkinan pengeluaran Anda.

Mengapa ada minimum: Memukul batas pengeluaran adalah pengalaman yang mengganggu. Minimum ada untuk membuatnya tidak mungkin bahwa variasi normal dalam penggunaan Anda akan menyebabkan mencapai batas pengeluaran.

Bagaimana estimasi konservatif dihitung: Perkiraan didasarkan pada aktivitas Anda dari bulan ke saat ini, tetapi ini bukan ekstrapolasi linier yang ketat. AWS melihat pengeluaran Anda hingga saat

ini dan sumber daya yang saat ini Anda jalankan. AWS juga menggunakan aktivitas Anda dari bulan sebelumnya — jika itu tinggi, itu menjadi minimum.

Jika Anda memiliki banyak sumber daya yang berjalan: Perkiraan konservatif dari kemungkinan pengeluaran Anda akan tinggi. Jika Anda ingin menetapkan batas pengeluaran yang lebih rendah, Anda harus menghentikan sumber daya tersebut terlebih dahulu.

Jika Anda mengaktifkan kembali proyek yang dijeda: Perkiraan konservatif dari kemungkinan pengeluaran Anda adalah pengeluaran Anda hingga saat ini selama sebulan ditambah penggunaan apa pun yang tidak dikenakan biaya.

> **Note**
>
> Batas pengeluaran tidak termasuk kredit dan berlaku untuk biaya sebelum pajak.

Notifikasi

Anda akan menerima pemberitahuan ketika biaya aktual mencapai 50%, 75%, dan 90% dari batas Anda, atau ketika Anda berada di jalur untuk mencapai atau melampaui batas pengeluaran Anda dalam 10 hari ke depan.

Sesuaikan pengaturan batas pengeluaran Anda dengan kontrol biaya awal opsional

Batas pengeluaran Anda membuat tagihan Anda tidak tumbuh melewati jumlah yang Anda tetapkan. Jika penggunaan Anda mencapai itu, AWS jeda sumber daya Anda untuk melindungi Anda. Kontrol opsional ini bertindak lebih awal dan lebih lembut, sehingga Anda tetap jauh di bawah batas.

Hentikan pembuatan sumber daya baru

Sekitar 7 hari sebelum Anda mencapai batas Anda, sumber daya baru berhenti diluncurkan. Ini dicapai melalui penerapan kebijakan pengendalian layanan yang dikelola oleh AWS. Kebijakan kontrol layanan tergantung pada layanan. Untuk melihat semua kebijakan kontrol layanan yang mungkin diterapkan pada proyek Anda, lihatKebijakan kontrol layanan untuk batas pengeluaran.

Semua sumber daya Anda yang sudah berjalan tetap berjalan. Dalam kebanyakan kasus, tidak ada yang Anda bangun terpengaruh. Namun, dalam beberapa kasus ini dapat menyebabkan pengalaman yang mengganggu. Misalnya, jika Anda telah mengaktifkan auto-scaling, dan jika kondisi terpenuhi untuk menjalankan tindakan ini, instance baru tidak akan diluncurkan.

Jeda sumber daya idle

Sekitar 5 hari sebelum Anda mencapai batas Anda, sumber daya idle dijeda. Aplikasi aktif Anda terus berjalan. Sumber daya idle dijeda berdasarkan rekomendasi oleh Compute AWS Optimizer. Untuk informasi selengkapnya, lihat Lihat rekomendasi idle.

Anda juga dapat melihat rekomendasi sumber daya idle Anda dengan masuk ke proyek Anda dan melihat peluang penghematan. Untuk informasi selengkapnya, lihat Pusat Pengoptimalan Biaya. Pada saat ini, sebagai bagian dari pengalaman batas pengeluaran Anda, kami akan secara otomatis menjeda EC2, RDS, dan titik akhir. SageMaker

Mengapa kami menjeda instans EC2: Kami menjeda instans EC2 jika pemanfaatan CPU puncak di bawah 5% dan jaringan I/O Anda kurang dari 5 MB per hari selama 14 hari terakhir.

Jika Anda memiliki tipe instans G atau P, ada kriteria idle yang berbeda. Jenis instans G atau P akan dijeda jika berikut ini benar selama 14 hari terakhir:

- GPU tidak beroperasi secara aktif selama lebih dari 99% periode lookback
- Enkoder GPU tidak digunakan untuk 99% atau lebih runtime instans
- Penggunaan memori GPU pada tingkat instans kurang dari 5%
- Penggunaan maksimum CPU kurang dari 5%
- Pemanfaatan jaringan kurang dari 5 MB/day

Mengapa kami menjeda database RDS: Kami menjeda RDS untuk MySQL dan RDS untuk PostgreSQL jika instance database bukan replika baca dan memiliki yang berikut selama 14 hari terakhir:

- Tidak ada koneksi database
- Penggunaan CPU rendah
- read/write Aktivitas rendah

Mengapa kami menjeda SageMaker titik akhir yang tidak aktif: Kami menjeda titik akhir jika SageMaker titik akhir tidak memiliki pemanggilan dalam 14 hari terakhir.

Jeda driver berbiaya tinggi

Sekitar 4 hari sebelum Anda mencapai batas Anda, biaya tertinggi yang menimbulkan sumber daya aktif dihentikan sementara. Ini bisa menjadi pengalaman yang mengganggu. Pada saat ini,

kami memilih sumber daya dari lima layanan ini: EC2, RDS, Lambda, Bedrock, dan. SageMaker Kontrol keikutsertaan ini dapat mencegah Anda mengeluarkan biaya jika Anda memiliki Lambda yang melarikan diri atau lonjakan Batuan Dasar yang tidak terduga.

Apa yang terjadi jika Anda mencapai batas Anda

AWS menjeda proyek Anda dan menghentikan semua sumber daya. Data Anda disimpan.

Untuk mengaktifkan kembali proyek Anda, tingkatkan batas pengeluaran Anda dari AWS Pengaturan. Setelah pengaktifan kembali, beberapa sumber daya mungkin perlu dimulai ulang secara manual.

> **Important**
>
> Jika Anda tidak mengambil tindakan dalam waktu 90 hari setelah proyek dijeda, akan menghapus data proyek AWS secara permanen.

Hal penting lainnya yang perlu diperhatikan

- Jika Anda menggunakan Amazon Route 53, Anda hanya dapat membeli satu domain setiap 24 jam. Anda harus memastikan bahwa biaya domain berada dalam batas pengeluaran, jika tidak, pembelian domain Anda tidak akan berhasil. Dalam kasus seperti itu, Anda harus meningkatkan batas pengeluaran sebelum melakukan pembelian.
- Anda dapat menerapkan batas pengeluaran hingga 10 proyek.

Buat batas pengeluaran di AWS Pengaturan

Untuk membuat batas pengeluaran di AWS Pengaturan

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Penagihan.
3. Dalam Biaya berdasarkan proyek, untuk batas Pengeluaran, pilih Tetapkan batas untuk proyek.
4. Anda dapat memilih batas pengeluaran yang disarankan atau batas khusus.
5. Jika Anda memilih batas khusus, masukkan jumlah kustom.
6. Pilih Tetapkan batas pengeluaran.
7. Untuk menyesuaikan batas pengeluaran Anda dengan kontrol biaya awal, Anda dapat memilih Hentikan peluncuran sumber daya baru, Jeda sumber daya idle, atau Jeda driver biaya teratas.

8. Pilih Hemat kontrol biaya awal.

Batas pengeluaran akan segera berlaku.

Perbarui batas pengeluaran di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Pemilik proyek dapat memperbarui batas pengeluaran di AWS Pengaturan kapan saja. Anda dapat menambah atau mengurangi batas pengeluaran, atau mengubah kontrol biaya awal opsional. Jika AWS telah memblokir peluncuran sumber daya baru atau menjeda sumber daya karena mendekati batas, Anda dapat meningkatkan batas pengeluaran Anda. Jika proyek Anda telah dijeda karena Anda mencapai batas, tingkatkan batas pengeluaran Anda untuk mengaktifkan kembali proyek Anda. Untuk informasi selengkapnya tentang cara kerja batas pengeluaran, lihatBuat batas pengeluaran di AWS Pengaturan.

Perbarui batas pengeluaran di AWS Pengaturan

Untuk memperbarui batas pengeluaran

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di Biaya berdasarkan proyek, untuk batas pengelu aran, pilih ikon pensil.
4. Untuk B atas pengeluaran bulanan (USD), masukkan batas pengeluaran baru.

   Kami memberikan rekomendasi berdasarkan pengeluaran Anda saat ini.
5. Untuk mengubah perlindungan yang Anda inginkan pada proyek Anda, pilih H entikan peluncuran sumber daya baru, Jeda sumber daya yang tidak aktif, atau Jeda driver berbiaya tertinggi.
6. Pilih Simpan pengaturan.

Perubahan batas pengeluaran akan segera berlaku.

Hapus batas pengeluaran di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Pemilik proyek dapat menghapus batas pengeluaran di AWS Pengaturan kapan saja. Ketika Anda menghapus batas pengeluaran, tidak AWS akan lagi memantau biaya Anda atau mengambil kontrol biaya awal pada proyek Anda. Untuk informasi selengkapnya tentang cara kerja batas pengeluaran, lihatBuat batas pengeluaran di AWS Pengaturan.

Hapus batas pengeluaran di AWS Pengaturan

Untuk menghapus batas pengeluaran

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di Biaya berdasarkan proyek, untuk batas pengelu aran, pilih ikon pensil.
4. Pilih Hapus batas.
5. Konfirmasikan pilihan Anda dan pilih Hapus.

Batas pengeluaran Anda akan segera dihapus.

Tingkat Gratis di baru kami AWS pengalaman

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat menggunakan Tingkat AWS Gratis untuk menjelajahi AWS layanan tanpa komitmen biaya. Jika Anda baru AWS, Anda menerima kredit USD $100 setelah Anda membuat akun, terlepas dari paket akun Anda. Anda juga dapat memperoleh hingga 100 USD tambahan di semua proyek

Anda dalam bentuk kredit dengan menyelesaikan aktivitas. Untuk informasi lebih lanjut tentang mendapatkan kredit tambahan, lihatDapatkan kredit tambahan. Selain itu, Anda memiliki akses ke lebih dari 30 AWS layanan gratis yang menawarkan batas penggunaan gratis bulanan.

Paket akun Gratis sangat ideal untuk pelanggan yang bereksperimen dengan AWS layanan dan membangun bukti konsep tanpa biaya hingga enam bulan. Anda tidak akan dikenai biaya apa pun selama periode ini sampai Anda meningkatkan ke paket akun berbayar. Paket akun gratis Anda berakhir setelah enam bulan atau ketika kredit Anda habis digunakan—mana yang terjadi lebih dulu. Selain itu, paket akun gratis tidak memiliki akses ke AWS layanan tertentu yang akan dengan cepat mengkonsumsi seluruh jumlah kredit Tingkat AWS Gratis, atau pembelian perangkat keras. Untuk daftar layanan yang memenuhi syarat pada paket akun gratis, lihat AWS Layanan yang didukung untuk Mendaftar AWS (baru).

Paket akun Berbayar sangat ideal untuk membangun aplikasi produksi yang berskala di luar jumlah kredit awal. Ketika penggunaan Anda melebihi saldo kredit Anda atau ketika Anda menggunakan layanan di mana kredit tidak berlaku, Anda membayar harga standar pay-as-you-go.

Semua proyek yang Anda miliki berada di bawah jenis rencana yang sama. Jika Anda meningkatkan ke paket akun Berbayar, semua proyek Anda memiliki akses ke layanan tambahan, dan Anda membayar harga bayar sesuai penggunaan standar untuk semua proyek. Untuk informasi selengkapnya, lihat Memutakhirkan akun Anda di AWS Pengaturan.

Anda dapat menggunakan Konsol Manajemen Biaya untuk melacak penggunaan Anda di semua AWS layanan yang menawarkan Tingkat Gratis untuk proyek Anda.

Melacak penggunaan Tingkat Gratis Anda

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

AWS Pemberitahuan penggunaan Tingkat Gratis secara otomatis memberi tahu Anda melalui email ketika Anda melebihi 85 persen dari batas Tingkat Gratis Anda untuk setiap layanan. Untuk pelacakan tambahan, Anda dapat mengonfigurasi untuk melacak penggunaan Anda hingga 100% dari batas Tingkat Gratis dengan menetapkan anggaran tanpa pengeluaran. Anda juga dapat memfilter anggaran Anda untuk melacak layanan individual.

Anda dapat melacak penggunaan AWS Tingkat Gratis Anda dengan cara berikut.

Penggunaan AWS Pengaturan

Anda dapat memantau tanggal kedaluwarsa paket akun gratis Anda, saldo kredit, dan hari yang tersisa di Peng AWS aturan. Untuk informasi selengkapnya, lihat Lihat dan tukarkan kredit di AWS Pengaturan. Anda juga menerima pemberitahuan email berkala mengenai saldo kredit Anda dan ketika Anda mendekati akhir periode paket akun gratis Anda.

Jika Anda memiliki paket berbayar, Anda dapat memantau saldo kredit dan tanggal kedaluwarsa Anda di halaman kredit di Peng AWS aturan. Untuk informasi selengkapnya tentang meningkatkan ke paket berbayar, lihatTingkatkan akun Anda di AWS Pengaturan.

Menggunakan Konsol Manajemen Penagihan dan Biaya

Anda dapat menggunakan Konsol Manajemen Penagihan dan Biaya untuk melacak penggunaan tingkat gratis di setiap proyek. Konsol Manajemen Penagihan dan Biaya menampilkan ringkasan penggunaan bulanan hingga saat ini dan penawaran layanan apa pun pada atau di atas batas penggunaan. Untuk setiap penawaran tingkat gratis yang digunakan, Anda dapat melihat yang berikut ini:

- Layanan
- B AWS atas penggunaan Tingkat Gratis
- Penggunaan Anda saat ini
- Prakiraan penggunaan Anda
- Penggunaan aktual bulan-ke-tanggal (MTD) Anda
- Prakiraan penggunaan bulan-ke-tanggal (MTD) Anda

Prosedur berikut menunjukkan cara menggunakan Konsol Manajemen Penagihan dan Biaya untuk mengurutkan penggunaan Tingkat Gratis berdasarkan penggunaan aktual bulanan hingga saat ini.

Untuk mengurutkan penggunaan Tingkat Gratis Anda

1. Buka Konsol Manajemen Penagihan dan Biaya di https://console.aws.amazon.com/cost-management/.
2. Pilih Tingkat Gratis.
3. Untuk mengurutkan berdasarkan penggunaan aktual bulan-ke-tanggal, pilih% penggunaan aktual MTD.

Dapatkan kredit tambahan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Jika Anda adalah AWS pelanggan baru, Anda dapat memperoleh tambahan kredit USD $100 terlepas dari rencana akun Anda dengan menyelesaikan aktivitas. Kegiatan-kegiatan ini membantu Anda mempelajari AWS layanan. Anda dapat menemukan aktivitas di AWS widget Jelajahi di dasbor Beranda AWS Konsol Anda. Semua aktivitas ini akan dikenakan biaya AWS layanan yang dikurangkan dari kredit Tingkat AWS Gratis Anda, namun ketika Anda menyelesaikan setiap aktivitas, Anda menerima kredit USD $20.

Kegiatan yang harus diselesaikan

- Luncurkan instans menggunakan Amazon EC2
- Gunakan model dasar di taman bermain Amazon Bedrock
- Buat anggaran
- Membuat aplikasi web menggunakan Lambda
- Buat database Amazon RDS

Lihat informasi penagihan Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat menggunakan Peng AWS aturan untuk melihat informasi penagihan Anda. Jika Anda menggunakan Tingkat Gratis, halaman ini menunjukkan berapa hari Tingkat Gratis yang Anda miliki dan AWS kredit Anda. Anda juga dapat melihat biaya per proyek. Jika Anda menggunakan Paket Berbayar, Anda dapat melihat saldo, biaya saat ini, dan biaya per proyek. Jika Anda menggunakan batas pengeluaran, Anda dapat melihat informasi yang terkait dengan batas Anda. Anda juga

bisa Kelola metode pembayaran Anda di AWS Pengaturan danKelola pendaftaran pajak di AWS Pengaturan.

Saat Anda menggunakan Paket Gratis, semua penggunaan ditanggung oleh kredit AWS Tingkat Gratis Anda. Anda perlu meningkatkan ke Paket Berbayar jika Anda menghabiskan kredit Tingkat AWS Gratis Anda atau setelah 184 hari, mana yang terjadi lebih dulu. Untuk informasi selengkapnya tentang meningkatkan ke Paket Berbayar, lihatTingkatkan akun Anda di AWS Pengaturan.

Untuk melihat biaya berdasarkan proyek

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di bawah Biaya berdasarkan proyek, Anda akan melihat biaya bulanan hingga saat ini dan perkiraan biaya bulan-ke-tanggal. Anda akan melihat semua biaya di seluruh proyek Anda.
4. (Opsional) Untuk melihat rincian biaya untuk proyek di bawah Per iksa biaya, pilih Lihat. Anda akan diarahkan ke konsol Pen AWS agihan dan Manajemen Biaya.

Data penagihan dan data Penjelajah Biaya yang Anda lihat di Konsol Manajemen Pen AWS agihan dan Biaya diperbarui setidaknya sekali sehari. Irama saat disegarkan mungkin berbeda. Jika Anda menggunakan batas pengeluaran, hal ini dapat menyebabkan perbedaan untuk perkiraan biaya bulanan hingga saat ini di Peng AWS aturan dan Konsol Manajemen AWS Biaya.

Lihat riwayat penagihan Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat melihat riwayat penagihan Anda di AWS Pengaturan. Riwayat penagihan Anda hanya tersedia jika Anda memiliki metode pembayaran. Jika Anda menggunakan Tingkat Gratis, Anda tidak akan melihat riwayat penagihan Anda.

Anda dapat mengunduh faktur untuk setiap penyedia layanan yang bertransaksi dengan Anda selama periode penagihan. Ini termasuk informasi seperti jenis tagihan, tanggal faktur, dan total

dalam USD. Jika faktur Anda diterbitkan dalam mata uang lain, total dalam mata uang lainnya juga ditampilkan. Faktur tidak dibagi di setiap proyek.

Untuk melihat riwayat penagihan Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di samping Sal do, pilih Lihat riwayat penagihan. Anda akan diarahkan ke riwayat penagihan.
4. Untuk mengunduh faktur, pilih ID faktur.

Kelola metode pembayaran Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat mengelola metode pembayaran Anda di Peng AWS aturan. Metode pembayaran Anda digunakan untuk membayar penggunaan AWS sumber daya di semua proyek Anda. Anda hanya dapat mengelola metode pembayaran jika Anda memberikan informasi saat membuat akun atau jika Anda meningkatkan akun Anda ke Paket Berbayar.

Untuk mengelola metode pembayaran Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di bawah Saldo, Anda akan melihat informasi pembayaran Anda. Pilih Kelola.
4. Untuk Metode pembayaran, pilih Per barui.
5. Masukkan metode pembayaran baru Anda dan pilih S impan.

Lakukan pembayaran di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat membayar AWS tagihan Anda di Peng AWS aturan. AWS membebankan biaya metode pembayaran default Anda secara otomatis pada awal setiap bulan. Jika tagihan tersebut tidak berhasil diproses, Anda dapat menggunakan konsol tersebut untuk memperbarui metode pembayaran Anda dan melakukan pembayaran.

Sebelum melakukan pembayaran, pastikan bahwa metode pembayaran yang Anda inginkan untuk ditagih secara otomatis di masa mendatang ditetapkan sebagai metode pembayaran default Anda. Jika Anda menggunakan kartu kredit, konfirmasikan bahwa kartu kredit Anda tidak kedaluwarsa.

Untuk melakukan pembayaran

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di samping Sal do, pilih Lihat riwayat penagihan. Anda akan diarahkan ke riwayat penagihan.
4. Di bawah Tindakan, Anda akan melihat B ayar faktur untuk setiap faktur yang belum dibayar. Jika tidak ada faktur yang terdaftar, Anda tidak perlu melakukan apa pun.
5. Pilih Bayar faktur.
6. Konfirmasikan pilihan Anda dan pilih Bayar.

Jika Anda memiliki pertanyaan tentang masalah dengan penagihan rekening bank Anda atau membayar saldo yang telah jatuh tempo, buat kasus di Pusat Dukungan.

Ubah mata uang pilihan Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat mengubah mata uang pilihan Anda di Peng AWS aturan. Mata uang pilihan Anda hanya berlaku untuk proyek yang Anda miliki. Negara penagihan tertentu membatasi mata uang pembayaran. Penerbit kartu Anda mungkin membebankan biaya untuk transisi dalam mata uang lain.

Untuk mengubah mata uang tampilan pilihan Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di bawah Saldo, Anda akan melihat informasi pembayaran Anda. Pilih Kelola. Jika Anda tidak melihat saldo, Anda tidak dapat mengubah mata uang.
4. Pilih Setel mata uang.
5. Untuk Mata uang pembayaran default, pilih mata uang pembayaran.
6. Pilih Simpan.

Kelola pendaftaran pajak di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda mengelola nomor registrasi pajak dan pembebasan pajak di Peng AWS aturan. Informasi pajak Anda hanya berlaku untuk proyek yang Anda miliki.

Memperbarui dan menghapus nomor pendaftaran pajak

Gunakan langkah-langkah berikut untuk memperbarui atau menghapus satu atau lebih nomor registrasi pajak.

> **Note**
>
> Jika suatu negara tidak terdaftar di menu tar ik- turun halaman pengaturan pajak, AWS tidak akan mengumpulkan pendaftaran pajak untuk negara tersebut saat ini.

Untuk memperbarui nomor pendaftaran pajak

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di bawah Saldo, Anda akan melihat informasi pembayaran Anda. Pilih Kelola.
4. Pilih Pengaturan pajak.
5. Ubah informasi pendaftaran pajak Anda.
6. Pilih Simpan.

Mengelola pembebasan pajak AS Anda

Jika negara bagian Anda memenuhi syarat, Anda dapat mengelola pembebasan pajak AS Anda di halaman Paket & penagihan di Peng AWS aturan. Dokumen yang Anda unggah untuk pengecualian akan ditinjau oleh Dukungan dalam waktu 24 jam. Anda hanya dapat mengelola pembebasan pajak jika akun Anda terdaftar sebagai bisnis.

Untuk mengunggah atau menambahkan pembebasan pajak AS Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di bawah Saldo, Anda akan melihat informasi pembayaran Anda. Pilih Kelola.
4. Pilih Kelola pembebasan pajak dan pilih Tambahkan pembebasan pajak.
5. Tentukan jenis pengecualian dan yurisdiksi Anda.
6. Unggah dokumen sertifikat.
7. Tinjau informasi Anda, dan pilih K irim.

Dalam waktu 24 jam, Dukungan akan memberi tahu Anda melalui kasus dukungan jika mereka memerlukan informasi tambahan, atau jika ada dokumen Anda yang tidak valid.

Setelah pengecualian disetujui, Anda dapat melihatnya di bawah tab Pembebasan pajak dengan masa berlaku Aktif.

Anda akan diberi tahu melalui kontak kasus dukungan jika pengecualian Anda ditolak.

Lihat dan tukarkan kredit di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Anda dapat melihat dan menukarkan kredit yang tersedia di Peng AWS aturan. AWS kredit secara otomatis diterapkan ke tagihan untuk membantu menutupi biaya yang terkait dengan layanan yang memenuhi syarat. Untuk informasi selengkapnya tentang layanan yang memenuhi syarat, lihat Men ebus Kredit AWS Promosi Anda. Kredit diterapkan di semua proyek yang Anda miliki sampai habis atau kedaluwarsa. Anda tidak dapat memilih proyek mana yang menggunakan kredit yang Anda tebus, kredit tersebut diterapkan di semua proyek yang Anda miliki.

Untuk melihat kredit Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di wadah biaya saat ini, Anda akan melihat kredit yang tersedia. Pilih kredit Anda.

   Anda akan diarahkan ke tampilan kredit aktif dan kedaluwarsa, atau kredit Anda dan kredit tidak aktif 6 bulan terakhir, tergantung pada jenis paket Anda.
4. Untuk melihat AWS layanan yang dapat digunakan dengan kredit Anda, pilih Lihat daftar layanan.

Untuk menebus AWS Kredit Promosi

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Pen agihan.
3. Di wadah biaya saat ini, Anda akan melihat kredit yang tersedia. Pilih kredit Anda.

   Anda akan diarahkan ke tampilan kredit aktif dan kedaluwarsa, atau kredit Anda dan kredit tidak aktif 6 bulan terakhir, tergantung pada jenis paket Anda.
4. Pilih Tukarkan kredit untuk menebus kredit Anda.

5. Untuk kode promosi, masukkan kode promosi seperti yang muncul. Saat Anda menebus kredit, Anda menunjukkan bahwa Anda telah membaca dan menyetujui Syarat dan AWS Ketentuan Kredit Promosi.
6. Pilih Tukarkan kredit.

Kelola akun di India di AWS Pengaturan

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Jika Anda mendaftar AWS dan memilih India untuk kontak dan alamat penagihan Anda, perjanjian pengguna Anda adalah dengan Amazon Web Services India Private Limited (AWS India), AWS penjual lokal di India. AWS India mengelola tagihan Anda, dan total faktur Anda tercantum dalam rupee India (INR), bukan dolar AS (USD).

Jika akun Anda AWS di India, ikuti prosedur dalam topik ini untuk mengelola akun Anda. Topik ini menjelaskan cara mendaftar untuk akun AWS India, mengedit informasi tentang akun AWS India Anda, mengelola verifikasi pelanggan, dan menambahkan atau mengedit Nomor Akun Permanen (PAN) Anda.

Topik

- Daftar untuk AWS (baru) dengan AWS India
- Mengelola informasi verifikasi pelanggan

Daftar untuk AWS (baru) dengan AWS India

AWS India adalah penjual lokal AWS di India. Jika kontak dan alamat penagihan Anda berada di India, gunakan prosedur berikut untuk mendaftar.

Untuk menggunakan Daftar untuk AWS (baru) dengan AWS India

1. Buka aws.amazon.com dan pilih Buat akun.
2. Pada spanduk yang menjelaskan perbedaan antara Mendaftar untuk AWS (baru) dan Mendaftar untuk AWS (lanjutan), pilih Daftar untuk AWS.

3. Pilih login seperti Google, Apple GitHub, atau Amazon.
4. Anda akan diarahkan ke login untuk penyedia Anda. Setelah Anda login, Anda akan diarahkan untuk AWS mendaftar.
5. Masukkan nama Anda dan pilih Lanjutkan.

   Nama ini akan dibagikan dengan anggota tim saat Anda memberi mereka akses ke proyek Anda.
6. Verifikasi email yang terkait dengan login Anda dengan memasukkan kode verifikasi. Ketika Anda telah memverifikasi email Anda, pilih Lanjutkan.
7. Masukkan kata sandi yang kuat untuk akun Anda dan pilih Lanjutkan.

   AWS mengharuskan kata sandi Anda memenuhi ketentuan berikut:

   - Itu harus memiliki minimal 8 karakter dan maksimal 128 karakter.
   - Ini harus mencakup minimal tiga dari campuran tipe karakter berikut: huruf besar, huruf kecil, angka, dan! @ # $% ^ portal manajemen * () <> [] {} | _+-= simbol.
   - Itu tidak boleh identik dengan Akun AWS nama atau alamat email Anda.
8. Masukkan detail kontak Anda dan pilih Lanjutkan.

   Jika kontak atau alamat penagihan Anda berbasis di India, sesuai dengan peraturan Tim Tanggap Darurat Komputer India (CERT-In), AWS diperlukan untuk mengumpulkan dan memvalidasi informasi identitas Anda sebelum memberi Anda akses ke layanan. AWS

   Nama yang Anda pilih antara kontak atau informasi penagihan harus sama persis dengan nama yang muncul pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen. Untuk daftar jenis dokumen yang diterima, lihatthe section called “Dokumen India yang diterima untuk verifikasi pelanggan”.
9. Pilih tujuan utama pendaftaran akun Anda.
10. Pilih jenis kepemilikan yang paling mewakili pemilik akun. Jika Anda memilih perusahaan, organisasi, atau kemitraan sebagai jenis kepemilikan, masukkan nama orang manajerial kunci. Orang manajerial utama dapat menjadi direktur, kepala operasi, atau orang yang bertanggung jawab atas operasi dalam bisnis Anda.
11. Bergantung pada jenis kepemilikan yang Anda pilih, pilih jenis dokumen India yang diterima untuk digunakan untuk verifikasi dan ketikkan informasi dokumen Anda.

> **Note**
>
> Jika Anda memiliki akun pribadi dan berencana untuk menggunakan SIM yang tidak dikeluarkan oleh Uni India, sebaiknya gunakan jenis dokumen pribadi yang berbeda untuk verifikasi.

12. Pilih nama yang ingin Anda gunakan untuk verifikasi pelanggan.

    Nama-nama dari informasi penagihan dan kontak Anda akan muncul untuk dipilih jika dikaitkan dengan alamat India. Pastikan nama yang Anda pilih cocok dengan nama pada jenis dokumen yang akan digunakan untuk verifikasi pelanggan. Jika Anda perlu membuat perubahan pada nama yang terkait dengan tagihan atau alamat kontak Anda, Anda dapat melakukannya setelah Anda menyelesaikan pendaftaran akun.

13. Berikan persetujuan Anda untuk mengirimkan informasi untuk verifikasi, lalu pilih Lanjutkan.

    Anda akan diberitahu tentang hasil verifikasi pelanggan melalui email setelah Anda menyelesaikan pendaftaran akun. Anda juga dapat memeriksa status pada halaman profil di AWS Pengaturan Saya. Anda harus lulus verifikasi pelanggan untuk mengakses AWS layanan.

14. AWS akan menyediakan proyek pertama Anda.

Untuk mengakses AWS Pengaturan, pilih Kelola proyek dari Konsol Manajemen AWS. Di AWS Pengaturan, Anda dapat mengundang anggota tim, membuat proyek baru, dan mengubah penagihan dan pengaturan lainnya.

Mengelola informasi verifikasi pelanggan

Sesuai dengan peraturan Tim Tanggap Darurat Komputer India (CERT-In), AWS diperlukan untuk mengumpulkan dan memvalidasi informasi identitas Anda sebelum memberi Anda akses baru atau berkelanjutan ke AWS layanan. Identitas Anda harus diverifikasi menggunakan nama dari tagihan India atau alamat kontak yang Anda berikan. Selama verifikasi, AWS akan memeriksa apakah nomor dokumen valid dan apakah nama yang Anda berikan cocok dengan nama yang terkait dengan dokumen yang Anda gunakan untuk verifikasi pelanggan. Nama yang Anda pilih antara kontak atau informasi penagihan harus sama persis dengan nama yang muncul pada dokumen.

Untuk memperbarui nama penagihan, alamat, dan informasi kontak lainnya, lihatGunakan AWS Pengaturan. Jika Anda mengedit informasi apa pun yang sebelumnya Anda gunakan untuk verifikasi

pelanggan, seperti nama atau India-based alamat dari informasi penagihan atau kontak Anda, Anda mungkin perlu memperbarui dan mengirimkan kembali informasi verifikasi pelanggan Anda.

Periksa status verifikasi pelanggan Anda

Anda dapat melihat status verifikasi pelanggan Anda kapan saja di halaman Kelola profil. Jika status verifikasi Anda diperlukan Verifikasi atau Verifikasi gagal, buat atau perbarui informasi verifikasi pelanggan Anda dan kirimkan untuk verifikasi.

Buat informasi verifikasi pelanggan Anda

Untuk menyelesaikan verifikasi pelanggan, Anda harus memberikan informasi dari dokumen India yang diterima. Untuk daftar jenis dokumen yang diterima, lihatthe section called “Dokumen India yang diterima untuk verifikasi pelanggan”.

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola profil.
3. Untuk verifikasi Pelanggan, pilih Buat verifikasi pelanggan.
4. Pilih nama yang sama persis dengan nama pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen.
5. Berikan informasi yang tersisa yang diminta di halaman. Bergantung pada jenis dokumen yang Anda pilih, Anda mungkin perlu mengunggah salinan bagian depan dan belakang dokumen. Jika Anda mengunggah file gambar, pastikan semua informasi dalam dokumen terlihat dan terbaca.
6. Pilih Kirim.

   Anda akan diberitahu tentang hasil verifikasi pelanggan dan langkah selanjutnya melalui email atau di Dasbor AWS Kesehatan.

Edit informasi verifikasi pelanggan Anda

Anda dapat mengedit informasi verifikasi pelanggan Anda, seperti tujuan utama pendaftaran akun, jenis organisasi Anda, dan nama, jenis dokumen, unggahan dokumen, atau informasi dokumen yang ingin Anda gunakan untuk verifikasi.

Jika Anda mengedit nama atau jenis dokumen yang akan digunakan untuk verifikasi pelanggan, atau memperbarui informasi dokumen apa pun, menyimpan perubahan akan mengharuskan identitas Anda diverifikasi lagi.

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kelola profil.
3. Untuk verifikasi Pelanggan, pilih Verifikasi Pelanggan.
4. Pilih Edit, lalu perbarui informasi yang ingin Anda ubah.

   Saat Anda memperbarui informasi, perhatikan panduan berikut:

   - Jika Anda memilih nama yang berbeda, nama harus sama persis dengan nama pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen.
   - Jika Anda memilih jenis dokumen yang berbeda, Anda perlu mengunggah salinan bagian depan dan belakang (jika ada) dokumen. Semua informasi dalam unggahan dokumen harus terlihat dan terbaca.
   - Jika Anda memiliki akun pribadi dan berencana untuk menggunakan SIM yang tidak dikeluarkan oleh Uni India, sebaiknya gunakan jenis dokumen pribadi yang berbeda untuk verifikasi.
   - Untuk daftar jenis dokumen yang diterima, lihatthe section called “Dokumen India yang diterima untuk verifikasi pelanggan”.
5. Pilih Kirim.

   Jika identitas Anda harus diverifikasi lagi karena jenis perubahan yang Anda simpan, Anda akan diberitahu tentang hasil verifikasi pelanggan dan langkah selanjutnya melalui email. Anda juga dapat melihat hasilnya dengan kembali ke halaman verifikasi Pelanggan atau di Dasbor AWS Kesehatan.

Dokumen India yang diterima untuk verifikasi pelanggan

Jenis dokumen berikut yang dikeluarkan oleh pemerintah India diterima untuk verifikasi pelanggan.

> **Note**
>
> Tautan yang dibagikan di bawah ini dapat berubah oleh pemerintah.

- Kartu PAN - Tersedia dalam format digital dan fisik, kartu Nomor Rekening Permanen (PAN) berisi pengidentifikasi alfanumerik unik yang dikeluarkan oleh Departemen Pajak Penghasilan India untuk individu, perusahaan, dan entitas. PAN terdiri dari sepuluh karakter, termasuk huruf dan angka, dalam format**`AAAAA1111A`**. Untuk menggunakan dokumen ini untuk verifikasi, Anda juga harus memberikan tanggal lahir (individu) atau tanggal pendirian (bisnis) yang muncul pada dokumen PAN dan mengunggah sisi depan kartu. Anda dapat mengunjungi situs web resmi Departemen Pajak Penghasilan untuk memeriksa validitas PAN Anda.
- ID Pemilih Card/EPIC - Kartu ID pemilih, juga dikenal sebagai Kartu Identitas Foto Pemilih (EPIC), berisi nomor identifikasi unik yang dikeluarkan oleh Komisi Pemilihan India untuk pemilih yang memenuhi syarat di India. ID/EPIC Nomor pemilih terdiri dari sepuluh karakter, termasuk huruf dan angka. Anda dapat mengunjungi situs resmi Komisi Pemilihan India untuk memeriksa validitas ID pemilih Anda. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus mengunggah sisi depan dan belakang kartu.
- Surat Izin Mengemudi - Jika SIM Anda tidak dikeluarkan oleh Uni India, kami sarankan menggunakan jenis dokumen yang berbeda untuk verifikasi. Nomor SIM terdiri dari 12-16 karakter, termasuk huruf, angka, dan spasi atau tanda hubung. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus memberikan tanggal lahir Anda dan mengunggah sisi depan dan belakang kartu. Anda dapat pergi ke situs Sewa Parivahan Kementerian Transportasi Jalan dan Jalan Raya untuk memeriksa validitas SIM Anda.
- Sertifikat Pendirian - Sertifikat pendirian adalah dokumen yang dikeluarkan oleh Kementerian Urusan Korporat (MCA) yang memberi tanggal pendaftaran bisnis sebagai badan hukum. Sertifikat ini digunakan untuk mengidentifikasi dan melacak perusahaan yang terdaftar di India secara unik. Setiap sertifikat berisi Corporate Identification Number (CIN), yang merupakan pengidentifikasi alfanumerik unik yang terdiri dari 21 karakter, termasuk huruf dan angka. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus mengunggah sertifikat dokumen pendirian. Anda dapat pergi ke portal Kementerian Urusan Korporat untuk memeriksa validitas CIN Anda.

Jenis dokumen India yang berbeda diterima untuk akun pribadi dan bisnis:

- Untuk akun pribadi - kartu PAN, ID pemilih card/EPIC, dan SIM.
- Untuk akun bisnis - kartu PAN dan sertifikat pendirian.

Siapkan penagihan India Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Jika Anda mendaftar AWS dan memilih India untuk alamat kontak dan penagihan Anda, perjanjian pengguna Anda adalah dengan Amazon Web Services India Private Limited (AWS India), pen AWS jual lokal di India. AWS India mengelola penagihan Anda, dan total faktur Anda terdaftar dalam rupee, bukan dolar. Semua informasi pajak hanya dapat dibuat atau dimodifikasi oleh pemilik proyek.

Untuk informasi pajak atau penagihan tambahan, Anda dapat menggunakan AWS Billing konsol untuk setiap proyek.

Gunakan bagian Paket & penagihan di halaman Kelola profil Peng AWS aturan untuk melakukan tugas-tugas berikut:

- Menambahkan atau mengedit Nomor Rekening Permanen
- Mengedit beberapa Nomor Rekening Permanen
- Mengedit beberapa nomor Pajak Barang dan Jasa
- Melihat faktur pajak

Menambahkan atau mengedit Nomor Rekening Permanen

Anda dapat menambahkan Nomor Akun Permanen (PAN) ke akun Anda dan mengeditnya.

Untuk menambahkan atau mengedit PAN

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil, lalu pilih Paket & penagihan.
3. Di bilah navigasi Pengaturan Pajak, memilih Mengedit.
4. Untuk Nomor Akun Tetap (PAN), memasukkan PAN Anda, lalu memilih Perbarui.

Mengedit beberapa Nomor Rekening Permanen

Anda dapat mengedit beberapa Nomor Akun Permanen (PAN) di akun Anda.

Untuk mengedit beberapa nomor PAN

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil, lalu pilih Paket & penagihan.
3. Di bawah Mengelola Nomor Pendaftaran Pajak, pilih nomor PAN yang ingin Anda edit.
4. Untuk Mengelola Pendaftaran Pajak, memilih Mengedit.
5. Perbarui bidang yang ingin Anda ubah, dan kemudian memilih Perbarui.

Mengedit beberapa nomor Pajak Barang dan Jasa

Anda dapat mengedit beberapa nomor Pajak Barang dan Jasa (GSTs) di akun Anda.

Mengedit beberapa nomor GST

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil, lalu pilih Paket & penagihan.
3. Di bawah Mengelola Nomor Pendaftaran Pajak, pilih nomor GST yang ingin Anda edit atau memilih Edit semuanya.
4. Untuk Mengelola Pendaftaran Pajak, memilih Mengedit.
5. Perbarui bidang yang ingin Anda ubah dan memilih Perbarui.

Melihat faktur pajak

Anda dapat melihat faktur pajak Anda di Peng AWS aturan.

Untuk melihat faktur pajak

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil, lalu pilih Paket & penagihan.
3. Gulir ke bawah dan pilih tab Faktur.
4. Di bagian Faktur pajak, pilih tautan faktur yang disebutkan di bawah ID Dokumen.

> **Note**
>
> Bagian Faktur pajak hanya muncul jika ada faktur pajak yang tersedia.

Mengubah penjual catatan ke atau dari AWS India

Anda dapat mengubah Akun AWS penjual catatan (SOR) Anda ke SOR lain dengan memperbarui informasi penagihan atau pajak Anda. Ini tidak berlaku jika akun AWS India Anda beroperasi dalam model lama di mana fungsinya tidak tersedia. Saat Anda mengedit negara atau wilayah dalam rincian penagihan atau pajak, SOR untuk akun Anda akan berubah secara otomatis jika penyedia layanan lokasi baru berbeda dari lokasi Anda saat ini.

Jika Anda mengubah akun ke atau dari AWS India, Anda tidak perlu memperbarui metode pembayaran default jika disetel ke faktur atau transfer bank. Jika metode pembayaran default Anda adalah kartu kredit atau debit, Anda diminta untuk mengonfirmasi kembali detail kartu pembayaran default Anda. Ini untuk memastikan metode pembayaran disimpan secara terpisah dari transaksi di luar AWS India. Untuk informasi selengkapnya, lihat Melihat kartu kredit atau debit yang memenuhi syarat untuk faktur AWS India.

> **Note**
>
> Jika Anda memiliki akun AWS India dengan kartu kredit atau debit sebagai metode pembayaran default Anda dan Anda telah menyiapkan mandat elektronik untuk pembayaran otomatis, Anda harus menonaktifkan mandat elektronik sebelum dapat mengedit preferensi pembayaran default Anda.

Untuk mengubah SOR akun Anda, Anda dapat mengedit informasi ini menggunakan opsi berikut:

Untuk mengubah SOR menggunakan informasi penagihan dan pajak

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil, lalu pilih Paket & penagihan.
3. Di bagian Preferensi pembayaran default, pilih Edit.
4. Masukkan alamat penagihan baru.

5. Di bagian Mata uang pembayaran, pilih mata uang default dari daftar mata uang yang diterima SOR baru Anda.
6. (Jika metode pembayaran default Anda adalah kartu kredit atau debit) Di bagian Konfirmasi metode pembayaran, masukkan kembali detail kartu pembayaran default Anda untuk mengonfirmasi penggunaan di bawah penyedia layanan baru.

   Untuk mengubah kartu default di bawah SOR baru, tambahkan kartu Anda di lain waktu dan ubah pengaturan metode pembayaran default Anda.
7. Pilih Simpan perubahan.

   Setelah beberapa menit, perubahan Anda termasuk SOR yang diperbarui muncul di halaman Preferensi Pembayaran.

Untuk mengubah SOR menggunakan informasi penagihan dan pajak

Untuk memindahkan akun Anda ke SOR yang berbeda, Anda harus memperbarui nomor registrasi pajak (TRN) yang terkait dengan akun dan memberikan TRN baru yang valid. Anda juga dapat menghapus TRN yang terkait dengan akun. SOR baru akun Anda secara otomatis diselesaikan berdasarkan negara alamat pajak baru Anda, dan alamat penagihan Anda saat ini, dalam urutan ketersediaan dan prioritas. Ketika SOR akun Anda berubah, Anda akan menerima pemberitahuan bahwa akun Anda pindah atau keluar dari AWS India.

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Kel ola profil, lalu pilih Paket & penagihan.
3. Pilih akun Anda dan pilih Kel ola pendaftaran pajak, lalu pilih Edit, E dit semua, atau H apus TRN.
4. (Jika metode pembayaran default Anda adalah kartu kredit atau debit) Di panel navigasi utama, pilih Kelola profil, lalu pilih Paket & penagihan.
5. Pilih Tambahkan metode pembayaran untuk memasukkan kembali detail kartu pembayaran default Anda, atau tambahkan kartu pembayaran baru.
6. Setelah kartu disimpan, pilih Tet apkan sebagai default.

   Bagian Preferensi pembayaran default memberi tahu Anda bahwa metode pembayaran default Anda sebelumnya tidak memenuhi syarat untuk digunakan di SOR baru. Segarkan halaman setelah Anda menambahkan kartu pembayaran agar peringatan ini hilang.

Akses AWS Support

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Ketika Anda mendaftar untuk AWS pengalaman baru kami, ada dua tempat di mana Anda dapat bekerja dengan AWS Support.

Anda dapat mengakses Dukungan Dasar atau Dukungan Bisnis+. Secara default, Anda terdaftar di Basic Support. Anda dapat memulai uji coba Dukungan Bisnis+untuk menggunakannya secara gratis hingga enam bulan.

Dukungan proyek

Jika Anda mengalami masalah dengan proyek, manajemen tim, atau masalah terkait penagihan, Anda dapat mengakses Dukungan Dasar atau Dukungan Bisnis+ di Pengaturan. AWS Anda dapat meminta proyek tambahan untuk organisasi Anda atau meminta peningkatan kuota terkait penagihan.

Untuk membuat kasus dukungan

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Support.
3. Untuk dukungan Proyek, pilih Buat kasus.
4. Untuk Subjek, masukkan subjek kasus dukungan Anda.
5. Untuk Deskripsi, jelaskan masalah Anda. Jika Anda bisa, jelaskan langkah-langkah untuk mereproduksi masalah.
6. Pilih Buat kasus.

Setelah Anda membuat kasus dukungan, Anda dapat melihat informasi kasus Anda untuk terus bekerja dengan dukungan.

Untuk melihat informasi kasus Anda

1. Buka AWS Pengaturan di https://settings.aws.com.

2. Di panel navigasi utama, pilih Support.
3. Pilih kasus dukungan Anda. Dalam tampilan ini Anda dapat melihat semua komunikasi tentang kasus Anda.
4. Untuk mengirim balasan ke dukungan, di Balas, masukkan balasan Anda dan kemudian pilih Kirim balasan.

Ketika kasus Anda teratasi, Anda dapat menyelesaikannya untuk menghapusnya dari AWS Pengaturan.

Untuk menyelesaikan kasus Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Support.
3. Pilih Resolve case (Selesaikan kasus).

Anda tidak akan dapat mengakses detail kasus setelah diselesaikan.

Dukungan teknis

Jika Anda mengalami masalah dengan AWS sumber daya Anda, Anda memerlukan dukungan teknis. Untuk mengakses dukungan teknis, buka kasus di AWS Support Center untuk proyek yang memiliki masalah.

Support jika semua proyek dan organisasi Anda ditutup

Jika semua proyek dan organisasi Anda ditutup, hubungi dukungan dengan mengisi formulir Support Feedback.

Di bagian Permintaan informasi, di bawah Bagaimana kami dapat membantu Anda, sertakan bahwa Anda menggunakan AWS pengalaman baru kami dan bahwa semua proyek Anda ditutup.

Mulai uji coba Dukungan Bisnis+

Anda bisa mendapatkan Dukungan Bisnis+gratis hingga enam bulan. Dukungan Bisnis+disediakan tanpa biaya hingga 31 Oktober 2026. Mulai 1 November 2026, harga standar dimulai dan Anda akan menerima $174 dalam kredit Dukungan Bisnis+untuk menutupi hingga enam bulan sebesar USD $29 per bulan. Anda tetap berlangganan ketika periode bebas berakhir dan kredit dimulai, dan AWS memberi tahu Anda ketika saldo kredit Anda hampir habis sebelum penagihan harga penuh dimulai.

Biaya Dukungan Bisnis+Anda adalah $ 29/month atau persentase dari AWS pengeluaran Anda, mana yang lebih besar. Untuk informasi lebih lanjut, lihat detail harga. Paket Anda diperbarui setiap bulan hingga Anda membatalkan.

Untuk memulai uji coba Dukungan Bisnis+Anda

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Support.
3. Pilih Mulai uji coba. Ini akan mempengaruhi semua proyek di organisasi Anda.
4. Tinjau persyaratan, pilih kotak centang perjanjian, lalu pilih Mulai uji coba.

Anda dapat membatalkan kapan saja tanpa komitmen dan tanpa penalti. Ketika Anda membatalkan, akses Dukungan Bisnis+segera berakhir dan kredit yang tidak digunakan akan hangus. Anda dapat mendaftar ulang dengan harga standar kapan saja, tetapi penawaran promosi Dukungan Bisnis+tidak dapat dipulihkan setelah dibatalkan.

Untuk membatalkan Dukungan Bisnis+

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Support.
3. Pilih Batalkan paket.
4. Pilih kotak centang untuk mengetahui bahwa pembatalan Dukungan Bisnis+mengembalikan Anda ke Dukungan Dasar segera, bahwa Anda akan kehilangan akses ke manfaat yang tercantum, dan bahwa $174 dalam kredit Anda akan dihapus dan tidak dapat dipulihkan.
5. Pilih Batalkan paket untuk kembali ke Dukungan Dasar.

Pantau proyek Anda menggunakan AWS CloudTrail

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Pantau proyek Anda menggunakan AWS CloudTrail

Proyek Anda terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh anggota tim atau AWS layanan. CloudTrail menangkap semua panggilan API untuk proyek Anda sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol dan operasi API untuk semua AWS layanan yang didukung. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk proyek Anda, orang yang membuat permintaan, kapan dibuat, dan detail tambahan.

Gunakan CloudTrail untuk melihat siapa yang memodifikasi proyek Anda

Tutorial ini untuk pengguna yang merasa nyaman dengan AWS CLI. Jika Anda berbagi proyek dengan beberapa anggota tim, Anda dapat menggunakan CloudTrail untuk melihat siapa yang memodifikasi sumber daya apa pun dalam proyek Anda. Setiap tindakan yang diambil oleh Anda atau anggota tim ketika mereka menggunakan AWS Pengaturan atau Konsol Manajemen AWS untuk mengakses proyek Anda dicatat oleh `onBehalfOf` parameter. Parameter ini menunjukkan ID pengguna dan ID penyimpanan identitas. Bersama-sama, nilai-nilai ini menentukan ID pembangun yang Anda undang untuk mengakses proyek Anda.

Untuk menemukan `onBehalfOf` parameter dan menghubungkannya ke anggota tim, Anda akan memerlukan akses ke AWS CLI dan file Konsol Manajemen AWS. Jika Anda tidak memiliki AWS CLI konfigurasi, Anda dapat menggunakan AWS CloudShell untuk mengakses shell pra-autentikasi berbasis browser yang dapat Anda luncurkan langsung dari perintah dan jalankan. Konsol Manajemen AWS AWS CLI

Langkah 1. Untuk menemukan AWS CloudTrail Event

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pada panel navigasi, pilih Riwayat peristiwa. Anda melihat daftar acara yang difilter, dengan acara terbaru ditampilkan terlebih dahulu. Pilih acara.
3. Dalam catatan acara, Anda akan melihat konten berikut:

```
"onBehalfOf": {
            "userId": "00000-e00f-000-000-0000000",
            "identityStoreArn":
 "arn:aws:identitystore::111122223333:identitystore/000000-0000-0000-0000-60000007"
}
```

Ini adalah identitas yang mendefinisikan anggota tim yang membuat CloudTrail acara.

Langkah 2. Untuk menghubungkan BehalfOf parameter on ke anggota tim

Untuk menghubungkan `onBehalfOf` parameter ke anggota tim menggunakan AWS CLI:

Untuk menggunakan AWS CLI di terminal Anda

1. Jalankan perintah berikut untuk masuk ke file AWS CLI. Anda dapat menemukan wilayah Anda menggunakanWilayah AWS untuk proyek Anda.

```
aws login --region project-region
```

2. Jalankan perintah berikut untuk mendapatkan ID untuk toko identitas Anda. CloudTrailAcara menunjukkan ARN toko identitas, tetapi tidak menunjukkan ID toko identitas. Anda selalu menggunakan Wilayah AWS `us-east-1` ketika menemukan ID untuk toko identitas Anda.

```
aws sso-admin list-instances --region us-east-1
```

Outputnya akan terlihat seperti berikut:

```
{
    "Instances": [
        {
            "InstanceArn": "arn:aws:sso:::instance/ssoins-0000000000",
            "IdentityStoreId": "d-000000",
            "OwnerAccountId": "111122223333",
            "CreatedDate": "2025-10-26T23:10:58.529000+00:00",
            "Status": "ACTIVE",
            "PrimaryRegion": "us-east-1",
            "Regions": [
                {
                    "RegionName": "us-east-1",
                    "Status": "ACTIVE",
                    "AddedDate": "2025-10-26T23:10:58.529000+00:00",
                    "IsPrimaryRegion": true
                }
            ]
        }
    ]
```

```
}
```

Anda ingin menyalin ID toko identitas. Dalam hal ini, ID toko identitas adalahd-000000.

3. Jalankan perintah berikut untuk menggambarkan anggota tim yang sesuai dengan onBehalfOf parameter.

```
aws identitystore describe-user --user-id 00000-e00f-000-000-0000000 --region us-
east-1 --identity-store-id d-000000
```

Outputnya akan terlihat seperti berikut:

```
{
    "IdentityStoreId": "d-000000",
    "UserId": "00000-e00f-000-000-0000000",
    "UserName": "carlos_salazar",
    "Name": {
        "FamilyName": "Salazar",
        "GivenName": "Carlos"
    },
    "DisplayName": "Carlos",
    "Emails": [
        {
            "Value": "carlos_salazar@example.com",
            "Type": "work",
            "Primary": true
        }
    ],
    "UserStatus": "ENABLED",
    "CreatedAt": "2025-10-26T23:15:27.213000+00:00",
    "CreatedBy": "00000000000",
    "UpdatedAt": "2025-10-26T23:18:55.432000+00:00",
    "UpdatedBy": "0000000000"
}
```

Nama tampilan dan email anggota tim Anda disediakan dalam output ini.

Untuk menghubungkan onBehalfOf parameter ke anggota tim menggunakan AWS CloudShell, masuk ke Konsol Manajemen AWS dan akses CloudShell. Untuk informasi selengkapnya, lihat Memulai dengan AWS CloudShell. Anda akan secara otomatis memiliki izin IAM yang benar untuk mengakses. CloudShell

Menutup proyek di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Jika Anda tidak lagi membutuhkan proyek Anda, Anda dapat menutupnya. Setelah Anda menutup proyek Anda, Anda dapat membukanya kembali dalam waktu 90 hari sejak Anda menutupnya. Waktu antara hari Anda menutup proyek dan ketika menutup proyek AWS secara permanen adalah periode pasca-penutupan.

Apa yang perlu Anda ketahui sebelum menutup proyek Anda

Sebelum Anda menutup proyek Anda, pertimbangkan hal berikut:

- Anda tidak dapat menutup proyek jika dijeda karena melebihi batas pengeluaran. Anda perlu mematikan batas pengeluaran dan kemudian menutup proyek. Untuk informasi selengkapnya, lihat Perbarui batas pengeluaran di AWS Pengaturan.
- Semua anggota tim akan secara otomatis kehilangan akses ke proyek ini dan semua sumber daya di dalamnya.
- Menutup proyek Anda akan berfungsi sebagai pemberitahuan penghentian Perjanjian AWS Pelanggan untuk proyek ini.
- Anda tidak perlu menghapus sumber daya dalam proyek Anda sebelum menutupnya. Namun, kami sarankan Anda membuat cadangan sumber daya atau data apa pun yang ingin Anda simpan. Untuk petunjuk tentang cara membuat cadangan sumber daya tertentu, lihat AWS dokumentasi yang sesuai untuk layanan tersebut.
- Anda dapat membuka kembali proyek Anda selama periode pasca-penutupan. Biaya untuk layanan yang tersisa di proyek Anda akan dimulai ulang jika Anda membukanya kembali. Anda juga tetap bertanggung jawab atas faktur yang belum dibayar.
- Anda tetap bertanggung jawab atas semua biaya dan biaya yang belum dibayar untuk layanan yang dikonsumsi sebelum penutupan proyek. Anda akan menerima AWS tagihan bulan berikutnya setelah menutup proyek Anda. Misalnya, jika Anda menutup akun Anda pada 15 Januari, Anda akan menerima tagihan pada awal Februari untuk penggunaan yang terjadi mulai 1 Januari hingga 15 Januari.

- Setelah proyek ditutup, AWS akan mengirim email harian hingga lima hari sebelum kami menangguhkan domain. Setelah domain ditangguhkan, dan tergantung pada pencatat domain, kami akan menghapus domain dalam waktu 30 hari atau melepaskan domain ke pencatat. Untuk informasi selengkapnya, lihat Domain saya Akun AWS ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53. Informasi ini ditulis untuk Akun AWS, tetapi informasinya akurat untuk proyek.
- AWS CloudTrail adalah layanan keamanan dasar. Ini berarti bahwa jejak yang dibuat oleh pengguna dapat terus ada dan mengirimkan acara bahkan setelah proyek ditutup, kecuali pengguna secara eksplisit menghapus jejak dalam proyek mereka sebelum menutupnya. Untuk informasi selengkapnya tentang cara meminta penghapusan jejak setelah ditutup, lihat Akun AWS penutupan dan jalur di Panduan CloudTrail Pengguna. Akun AWS Informasi ini ditulis untuk Akun AWS, tetapi informasi akurat untuk proyek.

Untuk menutup proyek

Untuk menutup proyek

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih proyek yang ingin Anda akses.
3. Untuk Tutup proyek, pilih Tutup proyek.
4. Konfirmasikan pilihan Anda dan pilih Tutup proyek.

Halaman proyek masih akan menampilkan proyek Anda selama 90 hari sampai dihapus secara permanen.

Post-closure periode

Periode pasca-penutupan mengacu pada lamanya waktu antara hari Anda menutup akun Anda dan saat menutup proyek Anda AWS secara permanen. Periode pasca-penutupan adalah 90 hari. Selama periode pasca-penutupan, Anda dapat mengakses konten dan AWS layanan hanya dengan membuka kembali proyek Anda. Setelah periode pasca-penutupan, AWS tutup proyek Anda secara permanen, dan Anda tidak dapat lagi membukanya kembali. AWS juga akan menghapus konten dan sumber daya di akun Anda (kecuali untuk CloudTrail jejak). Setelah proyek ditutup secara permanen, ID proyeknya tidak akan pernah dapat digunakan kembali.

Membuka kembali proyek Anda

Proyek Anda akan ditutup secara permanen dalam 90 hari, setelah itu Anda tidak akan dapat membuka kembali proyek Anda dan AWS akan menghapus konten yang tersisa di proyek Anda. Untuk membuka kembali proyek Anda sebelum ditutup secara permanen, (1) Anda harus menghubungi Dukungan sesegera mungkin, dan (2) kami harus menerima pembayaran penuh dari saldo yang belum dibayar, termasuk memberikan informasi yang diperlukan sebagaimana ditentukan pada faktur, dalam waktu 60 hari sejak tanggal penutupan akun.

> **Note**
>
> Biaya untuk layanan yang tersisa di proyek Anda akan dimulai ulang jika Anda membukanya kembali.

Aktifkan lanjutan AWS fitur

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Ketika Anda mengaktifkan fitur lanjutan, Anda mengambil kendali penuh atas AWS Organisasi, akun manajemen, dan akun administrator yang didelegasikan yang digunakan untuk mengelola proyek yang Anda buat dan anggota tim yang Anda undang. Anda akan langsung mengelola keamanan, tata kelola, dan keanggotaan tim di AWS lingkungan Anda. Anda memiliki akses ke AWS layanan tambahan, kemampuan Multi-wilayah, dan kontrol administratif dan penagihan yang ditingkatkan.

Anda harus memutakhirkan akun Anda sebelum mengaktifkan fitur-fitur lanjutan. Untuk informasi selengkapnya, lihat Tingkatkan akun Anda di AWS Pengaturan.

Apa yang terjadi ketika Anda mengaktifkan fitur-fitur canggih

Saat Anda mengaktifkan fitur-fitur lanjutan, perubahan berikut akan segera diterapkan ke akun manajemen Anda dan AWS Organisasi yang berisi proyek Anda:

- Anda sekarang adalah administrator AWS organisasi yang berisi proyek Anda.

- Anda menetapkan alamat email root untuk akun manajemen Anda. Anda juga harus mengatur kata sandi pengguna root. Untuk informasi selengkapnya, lihat Tetapkan kata sandi pengguna root untuk akun manajemen Anda.
- Anda mengelola proyek Anda sebagai akun anggota di organisasi Anda. Sebagai administrator organisasi ini, Anda dapat membuat akun anggota di organisasi. AWS Builder ID Anda terus memiliki akun project Anda. Untuk informasi selengkapnya, lihat Akun proyek setelah Anda mengaktifkan fitur lanjutan.
- Untuk memberikan akun anggota yang Anda undang untuk bergabung dengan organisasi Anda peran administrator, Anda harus membuat OrganizationAccountAccessRole. Untuk informasi selengkapnya, lihat Membuat akun anggota yang diundang. OrganizationAccountAccessRole
- Anggota tim Anda disebut sebagai identitas tenaga kerja dan mereka masih dapat mengakses akun Anda AWS . Anda juga dapat memilih untuk menyesuaikan sumber identitas tenaga kerja Anda menggunakan IAM Identity Center. Anda dapat terus menggunakan AWS Builder ID sebagai sumber identitas, atau Anda dapat mengubahnya menjadi sumber identitas eksternal. Jika Anda mengubah sumber identitas Anda dari AWS Builder ID ke sumber identitas lain, itu tidak dapat diubah. Anda tidak dapat mengaktifkan kembali AWS Builder ID sebagai sumber identitas di masa mendatang. Untuk informasi selengkapnya, lihat Mengubah sumber identitas dari AWS ID Pembangun.
- Anda mengontrol AWS akses untuk pengguna dan grup di instans organisasi Pusat Identitas IAM menggunakan Manajer akses akun. Anda dapat menggunakan fitur ini untuk memodifikasi akses pengguna, sambil tetap mengizinkan pengguna Anda untuk masuk menggunakan `aws login` untuk menerima kredensi sesi peran IAM mereka dari browser. Untuk informasi selengkapnya, lihat Manajer Akses AWS Akun.
- AWS membuat akun anggota yang disebut Admin Delegasi Identitas di organisasi Anda dengan peran administrator yang didelegasikan. Peran ini digunakan untuk melakukan sebagian besar tugas administratif di Pusat Identitas IAM dan manajer akses akun. Peran administrator yang didelegasikan harus digunakan di US East (Virginia N.). Untuk informasi selengkapnya, lihat Administrasi yang didelegasikan.

  ID AWS Builder Anda memiliki akun Admin Delegasi Identitas, seperti akun project Anda.
- Sekarang Anda dapat mengonfigurasi Kebijakan Kontrol Sumber Daya (RCP) dan Kebijakan Kontrol Layanan (SCP) untuk menerapkan pagar pembatas khusus di organisasi Anda. Sebelumnya, RCP dan SCP AWS terkelola atas nama Anda. Anda dapat mengubah kebijakan tersebut setelah mengaktifkan fitur-fitur lanjutan. Untuk informasi selengkapnya, lihat Hapus kebijakan organisasi.

Saat Anda mengaktifkan fitur lanjutan, perubahan berikut juga diterapkan ke AWS organisasi Anda:

- Jika Anda memiliki batas pengeluaran untuk salah satu AWS akun Anda, itu akan dihapus. Setiap proyek yang saat ini dijeda akan diaktifkan kembali. Anda tidak dapat membuat batas pengeluaran jika Anda mengaktifkan fitur-fitur canggih. Sebagai gantinya, Anda memiliki akses ke seluruh rangkaian Billing and Cost Management Tools. Ini termasuk mengatur anggaran, mengunduh laporan penjelajah biaya, dan mendeteksi pengeluaran yang tidak biasa dengan Deteksi Anomali AWS Biaya. Anda dapat menggunakan alat canggih ini untuk menganalisis, mengatur, merencanakan, dan mengoptimalkan biaya Anda.
- Anda dapat mengakses semua AWS layanan. Layanan yang tersedia tercantum dalamthe section called “Layanan AWS tidak didukung untuk yang baru AWS pengalaman”. Anda harus merencanakan arsitektur Anda dan berkonsultasi dengan dokumentasi layanan sebelum mengaktifkan layanan ini. Selain itu, Agen Toolkit menyediakan banyak keterampilan untuk bekerja dengan layanan ini.
- Anda mendapatkan akses ke Wilayah tambahan Wilayah AWS, ikut serta, dan akses ke kemampuan Multi-wilayah. Multi-Region arsitektur meningkatkan ketahanan untuk beban kerja Anda. Kami menyarankan Anda merencanakan bagaimana Anda akan membatasi dan mengaudit jejak regional Anda. Penting untuk memastikan bahwa sumber daya yang Anda buat hanya ada di Wilayah yang ingin Anda gunakan.
- Anda dapat menonaktifkan manajer peran IAM untuk masing-masing Akun AWS di organisasi Anda. Manajer peran IAM adalah pengaturan akun opsional yang secara otomatis menyediakan peran, sehingga Anda dan tenaga kerja Anda tidak perlu mengaturnya. Untuk informasi selengkapnya, lihat Cara mengaktifkan dan menonaktifkan manajer peran (konsol).
- Anda dapat menggunakan IAM Access Analyzer.

Saat Anda mengaktifkan fitur-fitur lanjutan, perubahan berikut juga diterapkan pada pengalaman pengguna Anda:

- Sebelumnya, Konsol Manajemen AWS menunjukkan tampilan yang disederhanakan dengan menu yang Anda gunakan untuk mengubah antara proyek dan mengakses AWS Pengaturan. Konsol Manajemen AWS Perluasan untuk menyertakan fitur tambahan seperti pemilih Wilayah, layanan tambahan, dan pengaturan warna untuk akun yang dapat Anda akses untuk membedakannya secara nyata. Untuk informasi selengkapnya, lihat Fitur konsol.
- Anda sekarang juga dapat melakukan hal berikut:
  - Nonaktifkan dukungan konsol multi-sesi.

- Tentukan AWS akun Anda sebagai HIPAA atau SEC compliant.
- Gunakan AWS Marketplace.
- Dapatkan kredit tambahan dari AWS Activate.
- Bekerja dengan Mitra AWS Pelatihan.
- Beli langganan Tim Pembuat AWS Keterampilan.
- Mendaftar dalam Perjanjian Perusahaan dengan AWS.
- Buat kontrak Layanan Profesional.
- Bergabunglah dengan Jaringan AWS Mitra.

Akun proyek setelah Anda mengaktifkan fitur lanjutan

Setiap proyek yang Anda buat di AWS Pengaturan berisi Akun AWS, yang disebut akun proyek. ID AWS Builder memiliki setiap akun proyek, bukan alamat email pengguna root. Ketika Anda mengaktifkan fitur lanjutan, akun project Anda menjadi akun anggota di organisasi Anda, dan AWS Builder ID Anda akan terus memilikinya, bahkan jika nanti Anda mengubah sumber identitas Anda. ID AWS Pembangun Anda juga memiliki akun Admin Delegasi Identitas yang AWS dibuat saat Anda mengaktifkan fitur-fitur lanjutan.

Karena akun proyek tidak memiliki alamat email pengguna root, ia bekerja secara berbeda dari akun anggota lain di organisasi Anda:

- Alamat email yang ditampilkan AWS Organizations konsol untuk akun proyek adalah placeholder yang AWS dihasilkan. `DescribeAccount`,, `ListAccounts` `ListAccountsForParent` `ListDelegatedAdministrators`, dan `GetPrimaryEmail` operasi mengembalikan placeholder yang sama. Ini bukan alamat email yang dapat Anda gunakan atau ubah.
- Anda tidak dapat memperbarui alamat email pengguna root dari akun proyek. Panggilan ke `StartPrimaryEmailUpdate` atau `AcceptPrimaryEmailUpdate` untuk akun proyek gagal dengan `AccessDeniedException` kesalahan, bahkan ketika pemanggil memiliki izin yang diperlukan.
- Anda tidak dapat masuk ke akun proyek sebagai pengguna root atau memulihkan kata sandi pengguna root.
- Anda tidak dapat menghapus akun proyek dari organisasi Anda, dan akun tersebut tidak dapat meninggalkan organisasi atau bergabung dengan organisasi lain. Jika Anda memanggil `RemoveAccountFromOrganization` akun proyek, panggilan gagal dengan

`ConstraintViolationException` kesalahan yang mengatakan akun tersebut dimiliki oleh Builder ID.

Untuk berhenti menggunakan akun proyek, tutup dari akun manajemen Anda. Karena Anda tidak dapat menghapus akun project dari organisasi, Anda dapat menghapus organisasi hanya setelah semua akun project Anda, termasuk akun Admin Delegasi Identitas, ditutup secara permanen. AWS menutup akun secara permanen ketika periode 90 hari pasca-penutupan berakhir.

Akun anggota yang Anda buat di organisasi setelah Anda mengaktifkan fitur lanjutan memiliki alamat email pengguna root, dan perbedaan ini tidak berlaku untuk mereka. Jika Anda memerlukan akun yang alamat email pengguna root dapat Anda ubah, atau yang dapat Anda hapus dari organisasi Anda nanti, buat akun anggota baru dan pindahkan sumber daya Anda ke sana.

Bagaimana akan AWS Pengaturan berubah setelah saya mengaktifkan fitur lanjutan?

Setelah Anda mengaktifkan fitur-fitur lanjutan, AWS Pengaturan akan tersedia selama Anda menggunakan AWS Builder ID sebagai sumber identitas Anda. AWS Pengaturan hanya akan dapat diakses dari https://settings.aws.com. Anda tidak akan dapat mengaksesnya dari Konsol Manajemen AWS. AWS Pengaturan akan menyediakan tautan untuk mengelola akun Anda menggunakan akun manajemen Anda. Dengan akun manajemen Anda, Anda dapat mengakses Konsol Manajemen AWS lokasi berikut dari AWS Pengaturan. Hanya gunakan akun manajemen untuk melakukan tugas administratif, termasuk:

- Akses Konsol Billing and Cost Management untuk melihat informasi penagihan Anda.
- Akses konsol AWS Organisasi untuk memodifikasi SCP dan RCP yang mengatur organisasi Anda.
- Akses konsol AWS Account Access Manager untuk memodifikasi akses butir halus untuk identitas tenaga kerja Anda.
- Akses Pusat Identitas IAM untuk mengubah sumber identitas Anda.

Gunakan akun manajemen untuk melakukan tugas-tugas ini. Meskipun Anda juga akan memiliki akses ke email pengguna root dan kata sandi, kami sarankan Anda hanya menggunakan kredenal pengguna root Anda untuk akses darurat ke akun Anda.

Anda juga dapat menggunakan AWS Pengaturan untuk mengakses AWS akun di organisasi, dan proyek apa pun yang dibagikan dengan Anda.

Jika Anda ingin membuat peran khusus dan mengaksesnya dari AWS Pengaturan di akun Anda, Anda harus mengatur durasi sesi menjadi 12 jam.

Jika Anda memiliki akses anggota tim ke proyek, Anda dapat melihat dan mengaksesnya dengan cara yang sama seperti sebelum Anda mengaktifkan fitur-fitur lanjutan. Setiap proyek yang dibagikan dengan Anda tidak akan terpengaruh jika Anda mengaktifkan fitur lanjutan untuk akun dan AWS organisasi manajemen Anda sendiri.

Bisakah saya masih membuat proyek di AWS Pengaturan setelah saya mengaktifkan fitur-fitur canggih?

Anda tidak dapat membuat proyek di AWS Organisasi saat ini setelah mengaktifkan fitur-fitur lanjutan. Anda harus membuat akun anggota di organisasi Anda.

Anda dapat membuat AWS Organisasi terkelola baru dengan default yang telah dikonfigurasi sebelumnya. Untuk melakukan ini, buat proyek baru di AWS Pengaturan. Anda kemudian dapat membuat proyek tambahan dan mengundang anggota tim untuk berkolaborasi. Anda dapat mengaktifkan fitur-fitur canggih untuk akun manajemen ini juga.

Lingkungan baru yang telah dikonfigurasi sebelumnya yang Anda akses tidak akan memiliki koneksi ke AWS organisasi sebelumnya yang dibuat saat Anda pertama kali mendaftar AWS.

Cara mempersiapkan untuk mengaktifkan fitur-fitur canggih

Sebaiknya lakukan hal berikut sebelum Anda mengaktifkan fitur-fitur lanjutan:

- Beri tahu semua anggota tim Anda bahwa Anda akan mengaktifkan fitur-fitur canggih. Kecuali Anda mengubah pengaturan apa pun, anggota tim Anda akan memiliki akses yang sama ke proyek, tetapi Konsol Manajemen AWS perubahan dari tampilan yang disederhanakan ke tampilan yang menunjukkan Wilayah dan menyediakan akses ke lebih banyak layanan. Jika nanti Anda mengubah sumber identitas atau menambahkan SCP atau RCP baru, beri tahu tenaga kerja Anda karena perubahan tersebut dapat memengaruhi cara mereka masuk dan apa yang dapat mereka akses.
- Lihat pengeluaran untuk semua proyek Anda saat ini dan perhatikan apakah ada proyek yang mengandung biaya yang berfluktuasi secara signifikan. Tanpa batas pengeluaran, Anda akan bertanggung jawab atas semua biaya yang dikeluarkan oleh sumber daya Anda. Sebaiknya hapus atau jeda sumber daya idle sebelum mengaktifkan fitur-fitur lanjutan.
- Rencanakan perubahan apa yang akan Anda buat untuk AWS organisasi Anda dan teliti praktik terbaik. Jika Anda berencana membuat sumber daya yang berbeda Wilayah AWS, ubah kebijakan

kontrol layanan yang diterapkan untuk dibatasi Wilayah AWS oleh semua pengguna. Anda perlu memodifikasi StateMentid `RegionFloor` untuk menyertakan Wilayah baru apa pun. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan untuk proyek.

- Jika Anda mengikuti langkah-langkahnyaHubungkan alat pengkodean AI, alat AI Anda hanya memiliki konteks tentang AWS pengalaman baru. Ini dapat menyebabkan masalah saat Anda mengembangkan menggunakan fitur-fitur canggih. Sebaiknya lakukan hal berikut:
  - Hapus `aws-starter-rules.md` file dari lokasi yang Anda simpan. File aturan disimpan tergantung pada agen Anda. Untuk informasi selengkapnya, lihat Tempat meletakkan file aturan.

Cara mengaktifkan fitur-fitur canggih

Anda dapat mengaktifkan fitur-fitur lanjutan di AWS Pengaturan. Aktivasi tidak dapat dibalik.

Untuk mengaktifkan fitur-fitur canggih

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Proyek.
3. Untuk Tindakan, pilih Jelajahi fitur lanjutan.

   Karena aktivasi tidak dapat dibalik, kami akan memberikan lebih banyak waktu untuk mengeksplorasi dan mempelajari tentang proses aktivasi.
4. Ketika Anda siap untuk mengaktifkan, lakukan hal berikut:

   a. Untuk nama Tim, masukkan nama tim. Ini adalah nama instance IAM Identity Center yang digunakan untuk menyimpan identitas tenaga kerja Anda. Tenaga kerja Anda akan melihat nama ini.

   b. Untuk Pilih alamat email akun manajemen, pilih alamat email. Alamat email ini digunakan untuk mengakses akun manajemen dan melakukan tugas. Jika Anda menggunakan alamat email yang berbeda, email AWS Builder ID akan tetap memiliki akses ke akun manajemen dari AWS Pengaturan, selama Anda masih menggunakan AWS Builder ID sebagai sumber identitas Anda.

   c. Selesaikan proses verifikasi untuk alamat email akun manajemen.

   d. Pilih Tinjau dan selesaikan aktivasi.

   e. Konfirmasikan pilihan Anda dan pilih aktifkan. Jika Anda melakukan ini, Anda tidak dapat mengembalikan akun Anda.

Selamat, Anda telah mengaktifkan AWS fitur-fitur canggih!

Setelah Anda mengaktifkan fitur-fitur canggih

Setelah Anda mengaktifkan fitur-fitur canggih, Anda dapat melakukan hal berikut:

- Kelola anggota tenaga kerja
- Mengubah sumber identitas dari AWS ID Pembangun
- Hapus kebijakan organisasi
- Buat unit organisasi
- Aktifkan atau nonaktifkan Wilayah AWS di akun Anda
- Buat peran IAM

Tetapkan kata sandi pengguna root untuk akun manajemen Anda

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Setelah Anda mengaktifkan fitur-fitur canggih, akun manajemen Anda sekarang menggunakan alamat email root untuk pemulihan akun. Meskipun Anda masih dapat memulihkan akses ke AWS Builder ID Anda menggunakan opsi layanan mandiri untuk memulihkan akses, Anda sekarang memulihkan akses ke akun manajemen Anda dengan kredensi pengguna root. Untuk mengakses pengguna root, Anda perlu membuat kata sandi pengguna root. Selain itu, kami menyarankan Anda mengaktifkan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan pengguna root Anda.

Untuk mengatur kata sandi pengguna root

1. Buka Konsol AWS Manajemen dan pilih Masuk menggunakan email pengguna root.
2. Untuk alamat Email, masukkan alamat email pengguna root.

   Ini adalah alamat email yang Anda tetapkan untuk akun manajemen saat Anda mengaktifkan fitur-fitur lanjutan.
3. Pilih Lupa kata sandi Anda?.

Proses reset kata sandi juga bagaimana Anda mengatur kata sandi pengguna root Anda setelah Anda mengaktifkan fitur-fitur lanjutan.

4. Masukkan alamat email yang terkait dengan akun.
5. Berikan teks CAPTCHA dan pilih Saya bukan robot.
6. Periksa email yang terkait dengan Anda Akun AWS untuk pesan dari Amazon Web Services. Email akan datang dari alamat yang berakhiran`@verify.signin.aws`. Ikuti petunjuk di email untuk mengatur kata sandi pengguna root. Jika Anda tidak melihat email di akun Anda, periksa folder spam Anda. Jika Anda tidak lagi memiliki akses ke email, lihat Saya tidak memiliki akses ke email untuk AWS akun saya di Panduan AWS Sign-In Pengguna.

Setelah Anda mengatur kata sandi pengguna root, Anda dapat memulihkan akses ke akun Anda. Selanjutnya, ikuti panduan dalam Multi-factor otentikasi untuk pengguna root AWS akun untuk mengaktifkan MFA untuk kredensi root Anda.

Hanya gunakan pengguna root untuk memulihkan akun Anda atau bila perlu untuk melakukan tugas yang memerlukan kredensi pengguna root. Untuk pekerjaan sehari-hari, masuk dengan sumber identitas Anda, seperti AWS Builder ID.

Kelola anggota tenaga kerja

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Setelah mengaktifkan fitur-fitur lanjutan, Anda dapat mengundang anggota tenaga kerja baru atau menghapus anggota tenaga kerja yang ada. Ini termasuk menambahkan tenaga kerja Anda yang ada ke AWS akun baru. Informasi berikut hanya untuk AWS organisasi yang menggunakan AWS Builder ID sebagai sumber identitas. Jika Anda menggunakan penyedia identitas eksternal (iDP), Anda mengelola tenaga kerja Anda di penyedia identitas tersebut. Jika Anda menggunakan direktori Pusat Identitas, gunakan dokumentasi yang dijelaskan dalam Kelola pengguna di direktori Pusat Identitas.

Mengundang anggota tenaga kerja baru

1. Buka AWS Pengaturan di https://settings.aws.com.

2. Di panel navigasi utama, pilih Proyek.
3. Kunjungi AWS konsol untuk akun admin yang didelegasikan identitas Anda.
4. Dari rumah AWS konsol, cari **`IAM Identity Center`** dan pilih.
5. Pada halaman Pengguna konsol Pusat Identitas IAM, pilih Undang anggota tim baru.
6. Untuk Email, masukkan alamat email atau daftar alamat email. Pisahkan alamat email dengan koma (,) atau titik koma (;).
7. Pilih Kirim undangan.

Untuk memberikan akses kepada anggota tenaga kerja baru AWS rekening

Setelah anggota tenaga kerja menerima undangan mereka, Anda mengonfigurasi AWS akun mana yang dapat mereka akses.

Berikan izin penuh ke akun yang Anda buat sebelum mengaktifkan fitur lanjutan

1. Identifikasi ID akun akun yang ingin Anda berikan aksesnya. Untuk menemukan ID akun, lihat Melihat pengenal AWS akun.
2. Di panel navigasi utama, pilih Grup.
3. Pilih nama grup yang dimulai dengan ID akun yang Anda identifikasi.
4. Pilih Tambahkan pengguna ke grup.
5. Pilih pengguna yang ingin Anda tambahkan.
6. Pilih Tambahkan 1 pengguna.

Berikan izin khusus ke yang baru atau yang sudah ada AWS akun

Anda mengonfigurasi akses kustom di Manajer Akses AWS Akun. Untuk informasi selengkapnya, lihat Mengelola akses ke AWS akun.

> **Note**
>
> Jika Anda ingin membuat peran khusus dan memberikan akses ke mereka dari AWS Pengaturan, Anda harus mengatur durasi sesi menjadi 12 jam.

Untuk menghapus anggota tenaga kerja

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Proyek.
3. Untuk Tindakan, pilih Kelola tim.

   Ini akan membuka Pusat Identitas IAM.
4. Pada halaman Pengguna konsol Pusat Identitas IAM, pilih anggota tim, lalu pilih Hapus.
5. Konfirmasikan pilihan Anda dan pilih Hapus.

Anggota tim akan segera kehilangan semua akses ke AWS organisasi Anda.

Langkah-langkah ini menunjukkan cara mengelola anggota tenaga kerja Anda dengan terlebih dahulu mengakses Pengaturan. AWS Namun, Anda dapat masuk ke Konsol Manajemen AWS dengan akun admin delegasi Anda dan mengakses Pusat Identitas IAM atau konsol IAM untuk mengelola anggota tenaga kerja Anda.

Mengubah sumber identitas dari AWS ID Pembangun

> **Warning**
>
> Saat ini kami merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Setelah mengaktifkan fitur-fitur lanjutan, Anda dapat mengubah sumber identitas Anda dari AWS Builder ID. Jika Anda mengubah sumber identitas dari AWS Builder ID, Anda tidak akan pernah dapat menggunakan kembali AWS Builder ID sebagai sumber identitas untuk AWS organisasi Anda. Mengubah sumber identitas Anda mengubah cara tenaga kerja Anda masuk. AWS Builder ID Anda terus memiliki akun project Anda.

Untuk mengubah sumber identitas Anda dari AWS ID Pembangun

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Proyek.
3. Di Kelola organisasi ini, pilih Ubah sumber identitas.

Ini akan membuka Pusat Identitas IAM.

4. Pada halaman Pengaturan konsol Pusat Identitas IAM, pilih Tindakan, lalu Ubah sumber identitas.
5. Untuk Pilih sumber identitas, AWS Builder ID akan dipilih. Pilih sumber baru dan kemudian pilih Berikutnya.
6. Jika Anda mengubah ke Active Directory, pilih direktori yang tersedia dari menu di halaman berikutnya. Jika Anda beralih ke penyedia identitas eksternal, kami sarankan Anda mengikuti langkah-langkah di Cara menyambung ke penyedia identitas eksternal.
7. Tinjau dan konfirmasikan perubahan Anda. Anda harus memilih semua kotak centang untuk mengonfirmasi bahwa Anda memahami perubahan pada organisasi Anda.
8. Konfirmasikan pilihan Anda dan pilih Ubah sumber identitas.

Langkah-langkah ini menunjukkan cara mengubah sumber identitas Anda dengan terlebih dahulu mengakses AWS Pengaturan. Namun, Anda dapat masuk ke akun admin delegasi Anda dan mengakses Pusat Identitas IAM untuk mengubah sumber identitas Anda. Konsol Manajemen AWS

Hapus kebijakan organisasi

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Setelah mengaktifkan fitur lanjutan, Anda dapat mengubah Kebijakan Kontrol Sumber Daya (RCP) dan Kebijakan Kontrol Layanan (SCP) untuk mengubah tata kelola organisasi Anda AWS . Kebijakan AWS organisasi terkelola tertentu dihapus saat Anda mengaktifkan fitur lanjutan. Untuk informasi selengkapnya, lihat Kebijakan terkelola untuk organisasi Anda. Informasi berikut hanya untuk AWS organisasi yang menggunakan AWS Builder ID sebagai sumber identitas. Jika Anda menggunakan sumber lain, ikuti langkah-langkah dalam Memperbarui kebijakan.

Untuk mengubah kebijakan kontrol layanan (SCP)

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Proyek.

3. Di Kelola organisasi ini, pilih Kelola kebijakan.

   Ini akan membuka AWS Organizations konsol.
4. Pilih halaman kebijakan kontrol layanan.
5. Pilih nama kebijakan yang ingin Anda perbarui.
6. Pada halaman detail kebijakan, pilih Edit kebijakan.
7. Membuat salah satu atau semua perubahan berikut:

   - Anda dapat mengubah nama kebijakan dengan memasukkan nama baru di Nama kebijakan.
   - Anda dapat mengubah deskripsi dengan memasukkan teks baru di Deskripsi kebijakan.
   - Anda dapat mengedit teks kebijakan dengan mengedit kebijakan dalam format JSON yang ada di panel kiri. Atau, Anda dapat memilih pernyataan di editor di sebelah kanan, dan juga mengubah elemen-elemennya dengan menggunakan kontrol. Untuk detail selengkapnya tentang setiap kontrol, lihat bagian Membuat prosedur SCP sebelumnya dalam topik ini.
8. Setelah Anda selesai, pilih Simpan perubahan.

Untuk mengubah kebijakan kontrol sumber daya (RCP)

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Proyek.
3. Di Kelola organisasi ini, pilih Kelola kebijakan.

   Ini akan membuka AWS Organizations konsol.
4. Pilih halaman kebijakan kontrol sumber daya.
5. Pilih nama kebijakan yang ingin Anda perbarui.
6. Pada halaman detail kebijakan, pilih Edit kebijakan.
7. Membuat salah satu atau semua perubahan berikut:

   - Anda dapat mengubah nama kebijakan dengan memasukkan nama baru di Nama kebijakan.
   - Anda dapat mengubah deskripsi dengan memasukkan teks baru di Deskripsi kebijakan.
   - Anda dapat mengedit teks kebijakan dengan mengedit kebijakan dalam format JSON yang ada di panel kiri. Atau, Anda dapat memilih pernyataan di editor di sebelah kanan, dan juga mengubah elemen-elemennya dengan menggunakan kontrol. Untuk detail selengkapnya tentang setiap kontrol, lihat prosedur Membuat RCP sebelumnya dalam topik ini.
8. Setelah Anda selesai, pilih Simpan perubahan.

Langkah-langkah ini menunjukkan cara memodifikasi kebijakan organisasi berdasarkan Peng AWS aturan. Namun, Anda dapat masuk Konsol Manajemen AWS dengan akun manajemen Anda dan mengakses AWS Organizations konsol untuk mengubah kebijakan ini.

Tutup akun Anda di AWS Pengaturan

> **Warning**
>
> Kami saat ini merilis pengalaman baru kami ke sejumlah pelanggan terbatas. Anda mungkin belum dapat mengakses pengalaman ini.

Jika Anda tidak lagi memerlukan organisasi dan semua proyek yang tersimpan di dalamnya, Anda dapat menutup proyek, menutup akun manajemen, dan menghapus ID AWS Builder Anda.

Untuk memastikan Anda tidak lagi dikenakan biaya untuk AWS sumber daya apa pun yang Anda konsumsi, Anda harus menutup proyek dan menutup akun manajemen untuk organisasi Anda, tetapi Anda tidak perlu menutup AWS profil Anda. ID AWS Builder Anda yang terkait dengannya gratis.

Setelah menutup akun manajemen, Anda dapat membukanya kembali dalam waktu 90 hari sejak Anda menutupnya. Waktu antara hari Anda menutup akun manajemen dan saat menutup akun manajemen AWS secara permanen adalah periode pasca-penutupan.

Apa yang perlu Anda ketahui sebelum menutup akun manajemen Anda

Sebelum menutup akun manajemen Anda, Anda harus mempertimbangkan hal-hal berikut:

- Saat Anda menutup proyek, pertimbangkan pertimbangannyaApa yang perlu Anda ketahui sebelum menutup proyek Anda.
- Anda harus menutup semua proyek sebelum Anda dapat menutup akun manajemen Anda.
- Anda harus menutup akun manajemen sebelum menghapus ID AWS Builder Anda.
- Setelah menutup akun manajemen, Anda dapat membukanya kembali dalam waktu 90 hari sejak Anda menutupnya. Waktu antara hari Anda menutup akun manajemen dan saat menutup akun manajemen AWS secara permanen adalah periode pasca-penutupan.
- Anda dapat membuka kembali akun Anda selama periode pasca-penutupan.
- Anda tidak dapat menggunakan alamat email yang sama yang terdaftar di organisasi Anda pada saat penutupan sebagai email utama organisasi lain. Jika Anda ingin menggunakan alamat email

yang sama untuk organisasi yang berbeda saat menggunakan Daftar untuk AWS (baru), sebaiknya perbarui sebelum penutupan. Untuk informasi selengkapnya, lihat Ubah alamat email Anda di AWS Pengaturan.

- Jika Anda telah mengaktifkan otentikasi multi-faktor (MFA) di akun manajemen dan mengonfigurasi perangkat MFA, MFA tidak dihapus secara otomatis saat Anda menutup akun manajemen. Jika Anda memilih untuk membiarkan MFA diaktifkan selama periode 90 hari pasca penutupan, pertahankan perangkat MFA aktif hingga periode pasca-penutupan berakhir jika Anda perlu mengakses akun selama waktu tersebut. Catatan, perangkat token TOTP perangkat keras tidak dapat dikaitkan dengan pengguna lain setelah penutupan permanen akun Anda. Jika Anda ingin menggunakan token TOTP perangkat keras dengan pengguna lain nanti, Anda memiliki opsi untuk menonaktifkan perangkat MFA perangkat keras sebelum menutup akun manajemen.

Menutup proyek

Untuk menutup proyek Anda, lihatMenutup proyek di AWS Pengaturan.

Tutup akun manajemen Anda

Untuk menutup akun manajemen

1. Buka AWS Pengaturan di https://settings.aws.com.
2. Di panel navigasi utama, pilih Project.
3. Untuk T ind akan, pilih Tutup akun manajemen.
4. Konfirmasikan pilihan Anda dan pilih Tutup akun manajemen.

Hapus Anda AWS ID Pembangun

Menghapus ID AWS Builder Anda akan menghasilkan hal berikut:

- Kehilangan akses: Selain proyek dan organisasi Anda, Anda tidak dapat lagi mengakses AWS alat dan layanan apa pun yang sebelumnya Anda akses melalui AWS Builder ID.
- Penghapusan konten: Konten yang tersisa yang terkait semata-mata dengan ID Pembuat Anda akan dihapus dan Anda tidak akan dapat lagi mengakses atau memulihkan konten Anda dari aplikasi menggunakan ID AWS Builder Anda. AWS
- Penghapusan informasi pribadi: Setiap informasi pribadi yang Anda berikan sehubungan dengan pembuatan dan administrasi ID Pem AWS bangun Anda akan dihapus, kecuali yang AWS dapat

menyimpan informasi pribadi sebagaimana diwajibkan atau diizinkan oleh hukum, seperti catatan permintaan penghapusan Anda atau data dalam bentuk yang tidak mengidentifikasi Anda.

Anda dapat mengetahui lebih lanjut tentang cara kami menangani informasi Anda di Pemberitahuan AWS Privasi. Anda dapat memperbarui preferensi AWS komunikasi atau berhenti berlangganan dengan mengunjungi Pusat P AWS referensi Komunikasi.

Login yang ada tetap tidak berubah — Jika Anda menggunakan login seperti Google atau Apple, menghapus ID AWS Builder Anda tidak menghapus apa pun yang terkait dengan akun login Anda.

Untuk menghapus AWS ID Pembangun

1. Buka AWS Pengaturan di https://settings.aws.com.

   Meskipun Anda telah menghapus akun manajemen Anda, Anda masih dapat masuk.
2. Di panel navigasi utama, pilih Kel ola profil.
3. Untuk Info Profil, pilih Kel ola profil.

   Anda akan diarahkan ke profil AWS Builder ID Anda.
4. Di panel navigasi utama, pilih Privasi & data.
5. Untuk Menghapus ID AWS Builder, pilih Hapus ID AWS Builder Anda.
6. Konfirmasikan pilihan Anda lalu pilih Hapus.

Daftar untuk AWS (lanjutan)

Jika Anda baru mengenal AWS, langkah pertama adalah mendaftar untuk Akun AWS. Saat Anda mengikuti informasi untuk Daftar AWS (lanjutan), AWS buat akun di mana Anda memiliki kendali penuh atas konfigurasi akun dan tempat konten Anda disimpan. Gunakan opsi ini jika Anda memiliki beban kerja yang diatur seperti HIPAA, FedRAMP.

Untuk membandingkan pendaftaran ini dengan Daftar untuk AWS (baru), lihatBandingkan opsi pendaftaran.

Untuk mendaftar Akun AWS, Anda harus memberikan informasi berikut:

- Alamat email pengguna root Alamat — Alamat email digunakan sebagai nama masuk untuk pengguna root dan diperlukan untuk pemulihan akun. Anda harus dapat menerima pesan email yang dikirim ke alamat ini. Sebelum Anda dapat melakukan tugas-tugas tertentu, Anda harus memverifikasi bahwa Anda memiliki akses ke email yang dikirim ke alamat ini.
- AWS Nama akun — Nama akun muncul di beberapa tempat, seperti pada faktur Anda, dan di konsol seperti dasbor Billing and Cost Management dan konsol. AWS Organizations Kami menyarankan Anda menggunakan cara standar untuk memberi nama akun Anda sehingga Anda dapat memberikan nama akun Anda yang mudah dikenali. Untuk akun perusahaan, pertimbangkan untuk menggunakan standar penamaan seperti organisasi - tujuan - lingkungan (misalnya, AnyCompany- audit - prod). Untuk akun pribadi, pertimbangkan untuk menggunakan standar penamaan seperti nama depan - nama belakang - tujuan (misalnya, paulo-santos-testaccount).
- Alamat - Jika kontak dan alamat penagihan Anda berada di India, perjanjian pengguna untuk akun Anda adalah dengan Amazon Web Services India Private Limited (AWS India), AWS penjual lokal di India. Anda harus memberikan CVV Anda sebagai bagian dari proses verifikasi. Anda mungkin juga harus memasukkan kata sandi satu kali, tergantung pada bank Anda. AWS India membebankan metode pembayaran Anda 2 INR sebagai bagian dari proses verifikasi. AWS India mengembalikan 2 INR setelah verifikasi selesai.
- Nomor telepon — Nomor ini digunakan untuk tujuan verifikasi identitas dan untuk mengkonfirmasi kepemilikan akun Anda. Anda harus dapat menerima panggilan dan pesan SMS di nomor telepon ini.

> **Important**
>
> Jika akun ini untuk bisnis, gunakan nomor telepon perusahaan sehingga perusahaan Anda dapat mempertahankan akses ke Akun AWS bahkan ketika seorang karyawan mengubah posisi atau meninggalkan perusahaan.

Langkah 1: Buat akun Anda

Instruksi ini untuk membuat Akun AWS bagian luar India. Untuk membuat akun di India, lihatBuat sebuah Akun AWS dengan AWS India. Untuk membuat akun yang merupakan bagian dari organisasi yang dikelola oleh AWS Organizations, lihat Membuat akun anggota di organisasi dalam Panduan AWS Organizations Pengguna.

Konsol Manajemen AWS

Untuk membuat sebuah Akun AWS

1. Buka AWS halaman Daftar untuk.
2. Masukkan alamat email pengguna root dan Akun AWS nama, lalu pilih Verifikasi alamat email. Ini mengirimkan kode verifikasi ke alamat email Anda.

   > **Important**
   >
   > Jika akun ini untuk bisnis, gunakan daftar distribusi perusahaan yang aman (misalnya,`it.admins@example.com`) sehingga perusahaan Anda dapat mempertahankan akses ke Akun AWS bahkan ketika seorang karyawan mengubah posisi atau meninggalkan perusahaan. Karena alamat email dapat digunakan untuk mengatur ulang kredensi pengguna root akun, lindungi akses ke daftar distribusi atau alamat ini.

3. Masukkan kode verifikasi Anda, lalu pilih Verifikasi.
4. Masukkan kata sandi yang kuat untuk pengguna root Anda, konfirmasikan, lalu pilih Lanjutkan. AWS mengharuskan kata sandi Anda memenuhi ketentuan berikut:

   - Itu harus memiliki minimal 8 karakter dan maksimal 128 karakter.

- Ini harus mencakup minimal tiga dari campuran tipe karakter berikut: huruf besar, huruf kecil, angka, dan! @ # $% ^ & * () <> [] {} | _+-= simbol.
- Itu tidak boleh identik dengan Akun AWS nama atau alamat email Anda.

5. Pilih paket akun Anda. Untuk informasi selengkapnya, lihat Paket Tingkat Gratis.
6. Masukkan informasi kontak Anda, lalu baca dan terima Perjanjian AWS Pelanggan. Pastikan Anda memahami persyaratan sebelum menerima.

> **Important**
>
> Jika akun ini untuk bisnis, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan daripada nomor untuk telepon pribadi. Mengkonfigurasi pengguna root akun dengan alamat email individual atau nomor telepon pribadi dapat membuat akun Anda tidak aman.

7. Masukkan informasi penagihan Anda. Jika Anda ingin menggunakan alamat penagihan yang berbeda untuk informasi AWS penagihan Anda, pilih Gunakan alamat baru.

   Anda tidak dapat melanjutkan proses pendaftaran sampai Anda menambahkan metode pembayaran yang valid.
8. Anda mungkin perlu mengkonfirmasi identitas Anda:

   a. Untuk kode Negara atau wilayah, masukkan nomor telepon yang dapat dihubungi dalam beberapa menit ke depan.

   b. Untuk nomor Telepon, masukkan nomor telepon yang dapat dihubungi dalam beberapa menit ke depan.

   c. Pilih Kirim SMS.

   d. Ketika sistem otomatis menghubungi Anda, masukkan kode yang Anda terima dan kemudian pilih Lanjutkan.
9. Pilih salah satu AWS Dukungan paket yang tersedia. Untuk penjelasan tentang paket Support yang tersedia dan manfaatnya, lihat Membandingkan Dukungan paket.
10. Pilih Daftar lengkap. Halaman konfirmasi muncul yang menunjukkan bahwa akun Anda sedang diaktifkan.
11. Periksa folder email dan spam Anda untuk pesan email yang mengonfirmasi akun Anda telah diaktifkan. Aktivasi biasanya memakan waktu beberapa menit tetapi terkadang bisa memakan waktu hingga 24 jam.

12. Setelah menerima pesan aktivasi, Anda dapat masuk ke untuk Konsol Manajemen AWSmulai menggunakan Layanan AWS. Untuk informasi umum tentang cara mengelola setelan akun, lihatKonfigurasikan Anda Akun AWS.

    Untuk beberapa yang Akun AWS dikelola melalui AWS Organizations, tetapkan akses administratif ke pengguna administratif di Pusat Identitas IAM. Untuk petunjuk, lihat Mengatur Akun AWS akses untuk pengguna administratif Pusat Identitas IAM di Panduan Pengguna Pusat Identitas IAM.

AWS CLI & SDKs

Anda dapat membuat akun anggota di organisasi yang dikelola AWS Organizations dengan menjalankan CreateAccountoperasi saat masuk ke akun manajemen organisasi.

Anda tidak dapat membuat mandiri Akun AWS di luar organisasi dengan menggunakan operasi AWS Command Line Interface (AWS CLI) atau AWS API.

Langkah 2: (Disarankan) Instal AWS CLI

Instal AWS CLI dengan mengikuti petunjuk di Instalasi AWS CLI. Anda memerlukan versi 2.32.0 atau yang lebih baru.

Anda dapat menggunakan AWS CLI untuk memiliki agen mengelola AWS sumber daya atas nama Anda.

Setelah Anda menginstal AWS CLI, gunakan perintah berikut untuk masuk secara terprogram:

```
aws login
```

Ini secara otomatis memutar kredensional Anda setiap 15 menit, menjaga sesi Anda tetap valid hingga 12 jam tanpa intervensi manual.

Gunakan perintah berikut untuk memverifikasi kredensional Anda berfungsi:

```
aws sts get-caller-identity
```

Untuk informasi selengkapnya tentang mengakses Anda Akun AWS, lihatMengakses Anda Akun AWS.

Langkah 3: (Disarankan) Siapkan AWS MCP Server

AWS MCP Server adalah server terkelola yang memberikan akses agen AWS melalui Model Context Protocol (MCP). Agen dapat mencari AWS dokumentasi dan mengambil informasi layanan tanpa otentikasi. Untuk menjalankan panggilan AWS API, jalankan skrip Python di lingkungan kotak pasir, atau ikuti keterampilan yang dikuratori, agen mengautentikasi melalui kredenal IAM Anda yang ada. Untuk informasi selengkapnya, lihat Apa itu Toolkit AWS Agen?

Setelah Anda menyelesaikan proses pendaftaran, lihat topik berikut:

- Terkait AWS layanan
- Menggunakan Pengguna root akun AWS
- Mengakses Anda Akun AWS
- Rencanakan Anda Akun AWS struktur tata kelola
- Konfigurasikan Anda Akun AWS
- Memecahkan masalah Anda Akun AWS
- Kelola akun di India
- Tutup Akun AWS
- Buka kembali Akun AWS

Terkait AWS layanan

Tergantung pada bagaimana Anda mendaftar AWS, Anda memiliki akses ke Akun AWS atau proyek. Proyek berisi Akun AWS dan pengaturan untuk berbagi dengan kolaborator lain. Untuk informasi selengkapnya, lihat Bandingkan opsi pendaftaran. Di bagian ini, kami menjelaskan cara Akun AWS Anda membuat menggunakan Daftar untuk AWS (lanjutan) bekerja dengan lancar dengan layanan berikut:

- IAM

  Anda Akun AWS terintegrasi erat dengan AWS Identity and Access Management (IAM). Anda dapat menggunakan IAM dengan akun Anda untuk memastikan bahwa orang lain yang bekerja di akun Anda memiliki akses sebanyak yang mereka butuhkan untuk menyelesaikan pekerjaan mereka. Anda juga menggunakan IAM untuk mengontrol akses ke semua sumber AWS daya Anda, tidak hanya informasi spesifik akun. Penting bagi Anda untuk membiasakan diri dengan konsep utama dan praktik terbaik IAM sebelum Anda terlalu jauh dengan menyiapkan struktur

Anda Akun AWS. Untuk informasi selengkapnya tentang administrator, lihat Praktik terbaik keamanan di IAM di dalam Panduan Pengguna IAM.

- AWS Organizations

  Jika perusahaan Anda besar atau cenderung tumbuh, Anda mungkin ingin membuat beberapa AWS akun yang mencerminkan struktur spesifik perusahaan Anda. AWS Organizations menyediakan infrastruktur dan kemampuan yang mendasari bagi Anda untuk membangun dan mengelola lingkungan multi-akun Anda. Anda dapat menggabungkan akun yang ada ke dalam organisasi yang memungkinkan Anda mengelola akun secara terpusat. Anda dapat membuat akun yang secara otomatis menjadi bagian dari organisasi Anda, dan Anda dapat mengundang akun lain untuk bergabung dengan organisasi Anda. Anda juga dapat melampirkan kebijakan yang memengaruhi sebagian atau semua akun Anda. Untuk informasi selengkapnya, lihat Kapan harus digunakan AWS Organizations.

  Tindakan API terkait akun berikut adalah bagian dari AWS Organizations API, bukan API Manajemen AWS Akun. Kami menyertakannya di sini karena pelanggan biasanya mencari operasi ini dalam dokumentasi Manajemen Akun, tetapi mereka didefinisikan dalam AWS Organizations namespace.

  - CreateAccount
  - CreateGovCloudAccount
  - DescribeAccount
- AWS Control Tower

  AWS Control Tower menyediakan cara yang disederhanakan untuk mengatur dan mengatur AWS lingkungan multi-akun yang aman. AWS Control Tower mengotomatiskan pembuatan lingkungan multi-akun Anda menggunakan AWS Organizations, membuat instance satu set akun awal dan dengan beberapa pagar pembatas default dan konfigurasi untuk lingkungan. Anda dapat menggunakan AWS Control Tower untuk menyediakan yang baru Akun AWS dalam beberapa langkah sambil memastikan bahwa akun sesuai dengan kebijakan organisasi Anda. Lihat informasi yang lebih lengkap di Kapan harus digunakan AWS Control Tower.

Menggunakan Pengguna root akun AWS

Tergantung pada bagaimana Anda mendaftar AWS, Anda memiliki akses ke Akun AWS atau proyek. Proyek berisi Akun AWS dan pengaturan untuk berbagi dengan kolaborator lain. Untuk informasi selengkapnya, lihat Bandingkan opsi pendaftaran. Di bagian ini, kami menjelaskan cara

menggunakan pengguna root dalam sebuah Akun AWS yang Anda buat menggunakan Daftar untuk AWS (lanjutan). ID AWS Builder memiliki setiap akun proyek, bukan alamat email pengguna root, sehingga Anda tidak dapat menggunakan pengguna root di akun proyek, termasuk setelah Anda mengaktifkan fitur lanjutan.

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Untuk menghindari penggunaan pengguna root untuk tugas sehari-hari, pelajari cara mengatur pengguna administratif AWS IAM Identity Center. Untuk rekomendasi keamanan pengguna root tambahan, lihat Praktik terbaik pengguna Root untuk Anda Akun AWS.

> **Important**
>
> Siapa pun yang memiliki kredensi pengguna root untuk Anda Akun AWS memiliki akses tidak terbatas ke semua sumber daya di akun Anda, termasuk informasi penagihan.

Anda dapat mengubah, atau mengatur ulang kata sandi pengguna root, dan membuat, atau menghapus kunci akses (ID kunci akses dan kunci akses rahasia) untuk pengguna root Anda. Untuk bantuan masuk menggunakan pengguna root Anda, lihat Masuk ke Konsol Manajemen AWS sebagai pengguna root di Panduan AWS Sign-In Pengguna.

Mengakses Anda Akun AWS

Informasi ini adalah tentang mengakses Anda Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Anda dapat mengakses Anda Akun AWS dengan salah satu cara berikut:

Konsol Manajemen AWS

Ini Konsol Manajemen AWS adalah antarmuka berbasis browser yang dapat Anda gunakan untuk mengelola Akun AWS pengaturan dan AWS sumber daya Anda.

AWS Alat Baris Perintah

Dengan alat AWS baris perintah, Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan Akun AWS dan AWS tugas. Dengan menggunakan baris perintah dapat lebih cepat dan lebih nyaman dibandingkan menggunakan konsol tersebut. Alat baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan AWS tugas. AWS menyediakan dua set alat baris perintah:

- AWS Command Line Interface(AWS CLI). Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat Panduan AWS Command Line Interface Pengguna.
- AWS Tools for Windows PowerShell. Untuk informasi tentang menginstal dan menggunakan Tools untuk Windows PowerShell, lihat Panduan Alat AWS untuk PowerShell Pengguna.

AWS SDK

AWS SDK terdiri dari pustaka dan kode sampel untuk berbagai bahasa pemrograman dan platform (misalnya, Java, Python, Ruby, .NET, iOS, dan Android). SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi selengkapnya tentang AWS SDK, termasuk cara mengunduh dan menginstalnya, lihat Alat untuk Amazon Web Services.

AWS Manajemen Akun HTTPS Query API

API Kueri HTTPS Manajemen AWS Akun memberi Anda akses terprogram ke Akun AWS dan AWS. API Kueri HTTPS memungkinkan Anda menerbitkan permintaan HTTPS secara langsung ke layanan. Saat Anda menggunakan HTTPS API, Anda harus menyertakan kode untuk menandatangani permintaan secara digital menggunakan kredensial Anda. Untuk informasi selengkapnya, lihat Memanggil API dengan membuat permintaan Kueri HTTP.

Rencanakan Anda Akun AWS struktur tata kelola

Informasi ini adalah tentang perencanaan struktur Akun AWS tata kelola Anda jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Meskipun Anda mungkin telah memulai AWS perjalanan Anda dengan satu akun, Anda disarankan AWS untuk menyiapkan beberapa akun seiring dengan bertambahnya ukuran dan kompleksitas beban kerja Anda. Apakah Anda bisnis menengah atau perusahaan besar, Anda pasti ingin membuat rencana struktur tata kelola yang akan memastikan data dan kebutuhan beban kerja Anda terpenuhi.

Bagian ini mencakup manfaat dan layanan tata kelola yang tersedia AWS untuk membantu mengaktifkan struktur tata kelola multi-akun.

Topik

- Manfaat menggunakan banyak Akun AWS
- Kapan harus digunakan AWS Organizations
- Kapan harus digunakan AWS Control Tower
- Memahami mode operasi API

Manfaat menggunakan banyak Akun AWS

Informasi ini adalah tentang manfaat menggunakan beberapa Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Akun AWS membentuk batas keamanan dasar di AWS Cloud. Mereka berfungsi sebagai wadah untuk sumber daya, menyediakan lapisan isolasi kritis yang penting untuk menciptakan lingkungan yang aman dan diatur dengan baik. Untuk informasi selengkapnya, lihat Apa itu Akun AWS?.

Memisahkan sumber daya menjadi terpisah Akun AWS membantu Anda mendukung prinsip-prinsip berikut di lingkungan cloud Anda:

- Kontrol keamanan — Aplikasi yang berbeda dapat memiliki profil keamanan yang berbeda, memerlukan kebijakan dan mekanisme kontrol yang berbeda di sekitarnya. Misalnya, jauh lebih mudah untuk berbicara dengan auditor dan dapat menunjuk ke satu Akun AWS yang menampung semua elemen beban kerja Anda yang tunduk pada Standar Keamanan Industri Kartu Pembayaran (PCI).
- Isol asi — An Akun AWS adalah unit perlindungan keamanan. Potensi risiko dan ancaman keamanan harus terkandung di dalam Akun AWS tanpa mempengaruhi orang lain. Mungkin ada kebutuhan keamanan yang berbeda karena tim yang berbeda atau profil keamanan yang berbeda.
- Banyak tim — Tim yang berbeda memiliki tanggung jawab dan kebutuhan sumber daya yang berbeda. Anda dapat mencegah tim mengganggu satu sama lain dengan memindahkannya untuk terpisah Akun AWS.
- Isolasi data — Selain mengisolasi tim, penting untuk mengisolasi penyimpanan data ke akun. Ini dapat membantu membatasi jumlah orang yang dapat mengakses dan mengelola penyimpanan

data tersebut. Ini membantu menahan paparan data yang sangat pribadi dan oleh karena itu dapat membantu sesuai dengan Peraturan Perlindungan Data Umum Uni Eropa (GDPR).

- Proses bisnis — Unit bisnis atau produk yang berbeda mungkin memiliki tujuan dan proses yang sama sekali berbeda. Dengan beberapa Akun AWS, Anda dapat mendukung kebutuhan spesifik unit bisnis.
- Penagihan — Akun adalah satu-satunya cara yang benar untuk memisahkan item pada tingkat penagihan. Beberapa akun membantu memisahkan item pada tingkat penagihan di seluruh unit bisnis, tim fungsional, atau pengguna individu. Anda masih bisa mendapatkan semua tagihan Anda dikonsolidasikan ke satu pembayar (menggunakan AWS Organizations dan tagihan konsolidasi) sambil memiliki item baris yang dipisahkan oleh Akun AWS.
- Alokasi kuota — kuota AWS layanan diberlakukan secara terpisah untuk masing-masing Akun AWS. Memisahkan beban kerja menjadi yang berbeda Akun AWS mencegah mereka mengonsumsi kuota satu sama lain.

Semua rekomendasi dan prosedur yang dijelaskan dalam dokumen ini sesuai dengan Ker AWS Well-Architected angka Kerja. Kerangka kerja ini dimaksudkan untuk membantu Anda merancang infrastruktur cloud yang fleksibel, tangguh, dan dapat diskalakan. Bahkan ketika Anda memulai dari yang kecil, kami sarankan Anda melanjutkan sesuai dengan panduan ini dalam kerangka kerja. Melakukan hal itu dapat membantu Anda menskalakan lingkungan Anda dengan aman dan tanpa memengaruhi operasi Anda yang sedang berlangsung saat Anda tumbuh.

Mengelola beberapa Akun AWS

Sebelum Anda mulai menambahkan beberapa akun, Anda harus mengembangkan rencana untuk mengelolanya. Untuk itu, kami sarankan Anda menggunakan AWS Organizations, yang merupakan AWS layanan gratis untuk mengelola semua Akun AWS di organisasi Anda.

AWS juga menawarkan AWS Control Tower, yang menambahkan lapisan otomatisasi AWS terkelola ke Organisasi dan secara otomatis mengintegrasikannya dengan AWS layanan lain seperti AWS CloudTrail AWS Config, CloudWatch, Amazon AWS Service Catalog,, dan lainnya. Layanan ini dapat menimbulkan biaya tambahan. Untuk informasi selengkapnya, lihat harga AWS Control Tower.

Lihat juga

- Kapan harus digunakan AWS Organizations
- Kapan harus digunakan AWS Control Tower

Kapan harus digunakan AWS Organizations

Informasi ini adalah tentang kapan harus digunakan AWS Organizations jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

AWS Organizations adalah AWS layanan yang dapat Anda gunakan untuk mengelola Anda Akun AWS sebagai grup. Ini menyediakan fitur seperti penagihan konsolidasi, di mana semua tagihan akun Anda dikelompokkan bersama dan ditangani oleh satu pembayar. Anda juga dapat mengelola keamanan organisasi secara terpusat dengan menggunakan kontrol berbasis kebijakan. Untuk informasi selengkap AWS Organizations nya, lihat Panduan AWS Organizations Pengguna.

Akses tepercaya

Bila Anda menggunakan AWS Organizations untuk mengelola akun sebagai grup, sebagian besar tugas administrasi untuk organisasi hanya dapat dilakukan oleh akun manajemen organisasi. Secara default, ini hanya mencakup operasi yang terkait dengan pengelolaan organisasi itu sendiri. Anda dapat memperluas fungsionalitas tambahan ini ke AWS layanan lain dengan mengaktifkan akses tepercaya antara Organisasi dan layanan tersebut. Akses tepercaya memberikan izin ke AWS layanan tertentu untuk mengakses informasi tentang organisasi dan akun yang dikandungnya. Saat Anda mengaktifkan akses tepercaya untuk Manajemen Akun, layanan Manajemen Akun memberikan izin kepada Organisasi dan akun manajemennya untuk mengakses metadata, seperti informasi kontak utama atau alternatif, untuk semua akun anggota organisasi.

Untuk informasi selengkapnya, lihat Aktifkan akses tepercaya untuk AWS Pengelolaan Akun.

Admin yang didelegasikan

Setelah mengaktifkan akses tepercaya, Anda juga dapat memilih untuk menetapkan salah satu akun anggota Anda sebagai akun admin yang dideleg asikan untuk Manajemen AWS Akun. Hal ini memungkinkan akun admin yang didelegasikan untuk melakukan tugas pengelolaan metadata Manajemen Akun yang sama untuk akun anggota di organisasi Anda yang sebelumnya hanya dapat dilakukan oleh akun manajemen. Akun admin yang didelegasikan hanya dapat mengakses tugas manajemen untuk layanan Manajemen Akun. Akun admin yang didelegasikan tidak memiliki semua akses administratif ke organisasi yang dimiliki akun manajemen.

Untuk informasi selengkapnya, lihat Aktifkan akun admin yang didelegasikan untuk AWS Pengelolaan Akun.

Kebijakan kontrol layanan

Ketika Anda Akun AWS adalah bagian dari organisasi yang dikelola oleh AWS Organizations, maka administrator organisasi dapat menerapkan kebijakan kontrol layanan (SCP) yang dapat membatasi apa yang dapat dilakukan oleh kepala sekolah di akun anggota. SCP tidak pernah memberikan izin; sebaliknya, ini adalah filter yang membatasi izin apa yang dapat digunakan oleh akun anggota. Pengguna atau peran (prinsi pal) dalam akun anggota hanya dapat melakukan operasi yang berada di persimpangan apa yang diizinkan oleh SCP yang berlaku untuk akun dan kebijakan izin IAM yang dilampirkan pada prinsipal. Misalnya, Anda dapat menggunakan SCP untuk mencegah prinsipal apa pun di akun memodifikasi kontak alternatif akun mereka sendiri.

Misalnya SCP yang berlaku untuk Akun AWS, lihatBatasi akses menggunakan AWS Organizations kebijakan kontrol layanan.

Aktifkan akses tepercaya untuk AWS Pengelolaan Akun

Petunjuk ini adalah tentang cara mengaktifkan akses tepercaya untuk Manajemen AWS Akun jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Mengaktifkan akses tepercaya untuk Manajemen AWS Akun memungkinkan administrator akun manajemen untuk mengubah informasi dan metadata (misalnya, detail kontak utama atau alternatif) khusus untuk setiap akun anggota di AWS Organizations. Untuk informasi selengkapnya, lihat Manajemen AWS Akun dan AWS Organizations di Panduan AWS Organizations Pengguna. Untuk informasi umum tentang cara kerja akses tepercaya, lihat Menggunakan AWS Organizations dengan AWS layanan lain.

Setelah akses tepercaya diaktifkan, Anda dapat menggunakan `accountID` parameter dalam operasi API Manajemen Akun yang mendukungnya. Anda dapat menggunakan parameter ini dengan sukses hanya jika Anda memanggil operasi menggunakan kredenSIAL dari akun manajemen, atau dari akun admin yang didelegasikan untuk organisasi Anda jika Anda mengaktifkannya. Untuk informasi selengkapnya, lihat Aktifkan akun admin yang didelegasikan untuk AWS Pengelolaan Akun.

Gunakan prosedur berikut untuk mengaktifkan akses tepercaya untuk Manajemen Akun di organisasi Anda.

Izin minimum

Untuk melakukan tugas-tugas ini, Anda harus memenuhi persyaratan berikut:

- Anda dapat melakukan ini hanya dari akun manajemen organisasi.

- Organisasi Anda harus mengaktifkan semua fitur.

Konsol Manajemen AWS

Untuk mengaktifkan akses tepercaya untuk AWS Pengelolaan Akun

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna root (tidak direkomendasikan) di akun pengelolaan organisasi.
2. Pilih Layanan di panel navigasi.
3. Pilih Manajemen AWS Akun dalam daftar layanan.
4. Pilih Aktifkan akses terpercaya.
5. Di kotak dialog Aktifkan akses tepercaya untuk Manajemen AWS Akun, ketik aktifkan untuk mengonfirmasinya, lalu pilih Aktifkan akses tepercaya.

AWS CLI & SDKs

Untuk mengaktifkan akses tepercaya untuk AWS Pengelolaan Akun

Setelah menjalankan perintah berikut, Anda dapat menggunakan kredenSIAL dari akun manajemen organisasi untuk memanggil operasi API Manajemen Akun yang menggunakan `--accountId` parameter untuk mereferensikan akun anggota dalam organisasi.

- AWS CLI: mengaktifkan akses layanan aws

  Contoh berikut memungkinkan akses tepercaya untuk Manajemen AWS Akun di organisasi akun panggilan.

```
$ aws organizations enable-aws-service-access \
    --service-principal account.amazonaws.com
```

  Perintah ini tidak menghasilkan output jika berhasil.

Aktifkan akun admin yang didelegasikan untuk AWS Pengelolaan Akun

Petunjuk ini adalah tentang cara mengaktifkan akun admin yang didelegasikan untuk Manajemen AWS Akun jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika

Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Anda dapat mendaftarkan satu akun admin yang didelegasikan per organisasi untuk layanan Manajemen AWS Akun. Setelah Anda mendaftarkan akun ini, pengguna dan peran dalam akun tersebut dapat memanggil operasi AWS CLI dan AWS SDK di `account` namespace yang dapat bekerja dalam mode Organisasi dengan mendukung `AccountId` parameter opsional. Ini memungkinkan admin yang didelegasikan untuk AWS memanggil operasi API Manajemen Akun untuk akun anggota lain di AWS Organizations.

Untuk mendaftarkan akun anggota di organisasi Anda sebagai akun admin yang didelegasikan, gunakan prosedur berikut.

AWS CLI & SDKs

Untuk mendaftarkan akun admin yang didelegasikan untuk layanan Manajemen Akun

Anda dapat menggunakan perintah berikut untuk mengaktifkan admin yang didelegasikan untuk layanan Manajemen Akun.

> **Izin minimum**
>
> Untuk melakukan tugas-tugas ini, Anda harus memenuhi persyaratan berikut:
>
> - Anda dapat melakukan ini hanya dari akun manajemen organisasi.
> - Organisasi Anda harus mengaktifkan semua fitur.
> - Anda harus mengaktifkan akses tepercaya untuk Manajemen Akun di organisasi Anda.

Anda harus menentukan prinsip layanan berikut:

```
account.amazonaws.com
```

- AWS CLI: daftar-administrator yang di delegasikan

  Contoh berikut mendaftarkan akun anggota organisasi sebagai admin yang didelegasikan untuk layanan Manajemen Akun.

  ```
  $ aws organizations register-delegated-administrator \
      --account-id 123456789012 \
  ```

```
    --service-principal account.amazonaws.com
```

Perintah ini tidak menghasilkan output jika berhasil.

Setelah menjalankan perintah ini, Anda dapat menggunakan kredenSIAL dari akun 123456789012 untuk memanggil operasi Account Management AWS CLI dan SDK API yang menggunakan `--account-id` parameter untuk mereferensikan akun anggota dalam suatu organisasi.

Konsol Manajemen AWS

Tugas ini tidak didukung di konsol manajemen Ac AWS count Management. Anda dapat melakukan tugas ini hanya dengan menggunakan operasi AWS CLI atau API dari salah satu AWS SDK.

Batasi akses menggunakan AWS Organizations kebijakan kontrol layanan

Informasi ini adalah tentang membatasi akses menggunakan kebijakan kontrol AWS Organizations layanan jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Topik ini menyajikan contoh yang menunjukkan bagaimana Anda dapat menggunakan kebijakan kontrol layanan (SCP) AWS Organizations untuk membatasi apa yang dapat dilakukan pengguna dan peran dalam akun di organisasi Anda. Untuk informasi selengkapnya tentang kebijakan kontrol layanan, lihat topik berikut di Panduan AWS Organizations Pengguna:

- Membuat SCP
- Melampirkan SCP ke OU dan akun
- Strategi untuk SCP
- Sintaks kebijakan SCP

Example Contoh 1: Mencegah akun memodifikasi kontak alternatifnya sendiri

Contoh berikut menolak operasi `PutAlternateContact` dan `DeleteAlternateContact` API agar tidak dipanggil oleh akun anggota mana pun dalam mode akun mandiri. Ini mencegah prinsipal apa pun di akun yang terkena dampak mengubah kontak alternatif mereka sendiri.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "arn:aws:account::*:account" ]
        }
    ]
}
```

Example Contoh 2: Mencegah akun anggota memodifikasi kontak alternatif untuk akun anggota lain di organisasi

Contoh berikut menggeneralisasi `Resource` elemen menjadi “*”, yang berarti bahwa itu berlaku untuk permintaan mode mandiri dan permintaan mode organisasi. Ini berarti bahwa bahkan akun admin yang didelegasikan untuk Manajemen Akun, jika SCP berlaku untuk itu, diblokir dari mengubah kontak alternatif apa pun untuk akun apa pun di organisasi.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "*" ]
        }
    ]
```

```
}
```

Example Contoh 3: Mencegah akun anggota di OU memodifikasi kontak alternatifnya sendiri

Contoh SCP berikut mencakup kondisi yang membandingkan jalur organisasi akun dengan daftar dua OU. Hal ini mengakibatkan pemblokiran prinsipal di akun mana pun di OU yang ditentukan dari memodifikasi kontak alternatif mereka sendiri.

Kapan harus digunakan AWS Control Tower

Informasi ini adalah tentang kapan harus digunakan AWS Control Tower jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

AWS Organizations adalah layanan dasar yang memungkinkan Anda untuk mengelola dan mengamankan seluruh AWS lingkungan Anda secara terpusat. Komponen penting dari pendekatan AWS Organizations sentris ini adalah AWS Control Tower. AWS Control Tower bertindak sebagai konsol manajemen dalam Organisasi, menyediakan cara yang efisien untuk mengatur dan mengatur AWS lingkungan multi-akun yang aman dengan menerapkan praktik terbaik preskriptif.

Pendekatan praktik terbaik keamanan ini disediakan oleh AWS Control Tower memperluas kemampuan inti AWS Organizations. AWS Control Tower menerapkan serangkaian pagar pembatas pencegahan dan detektif untuk membantu memastikan organisasi dan akun Anda tetap selaras dengan standar keamanan dan kepatuhan yang direkomendasikan.

Dengan membangun AWS Organizations struktur yang dirancang dengan baik AWS Control Tower, Anda dapat dengan cepat menerapkan lingkungan yang dapat diskalakan, aman, dan sesuai. AWS Pendekatan terpusat untuk manajemen dan tata kelola cloud ini sangat penting bagi perusahaan yang ingin memanfaatkan kekuatan penuh AWS Cloud sambil mempertahankan standar keamanan dan kepatuhan tertinggi.

Untuk informasi selengkapnya, lihat Apa itu AWS Control Tower? dalam Panduan Pengguna AWS Control Tower .

Memahami mode operasi API

Informasi ini adalah tentang memahami mode operasi API jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Operasi API yang bekerja dengan atribut Akun AWS an selalu bekerja di salah satu dari dua mode operasi:

- Konteks mandiri — mode ini digunakan ketika pengguna atau peran dalam akun mengakses atau mengubah atribut akun di akun yang sama. Mode konteks mandiri secara otomatis digunakan jika Anda tidak menyer takan `AccountId` parameter saat memanggil salah satu operasi Manajemen Akun AWS CLI atau AWS SDK.
- Konteks organisasi — mode ini digunakan ketika pengguna atau peran dalam satu akun dalam organisasi mengakses atau mengubah atribut akun di akun anggota yang berbeda di organisasi yang sama. Mode konteks organisasi secara otomatis digunakan ketika Anda menyer takan `AccountId` parameter saat memanggil salah satu operasi Manajemen Akun AWS CLI atau AWS SDK. Anda dapat memanggil operasi dalam mode ini hanya dari akun manajemen organisasi, atau akun admin yang didelegasikan untuk Manajemen Akun.

Oper AWS CLI asi dan AWS SDK dapat bekerja baik dalam konteks mandiri atau organisasi.

- Jika Anda tidak menyertakan `AccountId` parameter, maka operasi berjalan dalam konteks mandiri dan secara otomatis menerapkan permintaan ke akun yang Anda gunakan untuk membuat permintaan. Ini benar apakah akun tersebut adalah anggota organisasi atau tidak.
- Jika Anda menyertakan `AccountId` parameter, maka operasi berjalan dalam konteks organisasi, dan operasi bekerja pada akun Organisasi yang ditentukan.
  - Jika akun yang memanggil operasi adalah akun manajemen atau akun admin yang didelegasikan untuk layanan Manajemen Akun, maka Anda dapat menentukan akun anggota organisasi tersebut dalam `AccountId` parameter untuk memperbarui akun yang ditentukan.
  - Satu-satunya akun dalam organisasi yang dapat memanggil salah satu operasi kontak alternatif dan menentukan nomor akunnya sendiri dalam `AccountId` parameter adalah akun yang ditentukan sebagai akun admin yang di deleg asikan untuk layanan Manajemen Akun. Akun lain, termasuk akun manajemen, menerima `AccessDenied` pengecualian.
- Jika Anda menjalankan operasi dalam mode mandiri, maka Anda harus diizinkan untuk menjalankan operasi dengan kebijakan IAM yang menyertakan `Resource` elemen `"*"` untuk mengizinkan semua sumber daya, atau ARN yang menggunakan sintaks untuk akun mandiri.
- Jika Anda menjalankan operasi dalam mode organisasi, maka Anda harus diizinkan untuk menjalankan operasi dengan kebijakan IAM yang menyertakan `Resource` elemen `"*"` untuk mengizinkan semua sumber daya, atau ARN yang menggunakan sintaks untuk akun anggota dalam organisasi.

Memberikan izin untuk memperbarui atribut akun

Seperti kebanyakan AWS operasi, Anda memberikan izin untuk menambah, memperbarui, atau menghapus atribut akun Akun AWS dengan menggunakan kebijakan izin IAM. Saat Anda melampirkan kebijakan izin IAM ke prinsipal IAM (baik pengguna atau peran), Anda menentukan tindakan yang dapat dilakukan oleh kepala sekolah pada sumber daya mana, dan dalam kondisi apa.

Berikut ini adalah beberapa pertimbangan khusus Manajemen Akun untuk membuat kebijakan izin.

Format Nama Sumber Daya Amazon untuk Akun AWS

- Nama Sumber Daya Amazon (ARN) untuk Akun AWS yang dapat Anda sertakan dalam `resource` elemen pernyataan kebijakan dibuat secara berbeda berdasarkan apakah akun yang ingin Anda rujuk adalah akun mandiri atau akun yang ada di organisasi. Lihat bagian sebelumnya diMemahami mode operasi API.
  - Akun ARN untuk akun mandiri:

    ```
    arn:aws:account::{AccountId}:account
    ```

    Anda harus menggunakan format ini saat menjalankan operasi atribut akun dalam mode mandiri dengan tidak menyertakan `AccountID` parameter.
  - Akun ARN untuk akun anggota dalam suatu organisasi:

    ```
    arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
    ```

    Anda harus menggunakan format ini saat menjalankan operasi atribut akun dalam mode organisasi dengan menyertakan `AccountID` parameter.

Kunci konteks untuk kebijakan IAM

Layanan Manajemen Akun juga menyediakan beberapa kunci kondisi khusus layanan Manajemen Akun yang memberikan kontrol halus atas izin yang Anda berikan.

`akun: AccountResourceOrgPaths`

Kunci konteks `account:AccountResourceOrgPaths` memungkinkan Anda menentukan jalur melalui hierarki organisasi Anda ke unit organisasi tertentu (OU). Hanya akun anggota

yang terkandung oleh OU tersebut yang cocok dengan kondisi tersebut. Cuplikan contoh berikut membatasi kebijakan untuk diterapkan hanya pada akun yang ada di salah satu dari dua OU tertentu.

Karena `account:AccountResourceOrgPaths` merupakan tipe string multi-nilai, Anda harus menggunakan ForAnyValue atau operator string ForAllValues multi-nilai. Juga, perhatikan bahwa awalan pada kunci kondisi adalah`account`, meskipun Anda mereferensikan jalur ke OU dalam organisasi.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgPaths": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
        ]
    }
}
```

akun: AccountResourceOrgTags

Kunci konteks `account:AccountResourceOrgTags` memungkinkan Anda mereferensikan tag yang dapat dilampirkan ke akun dalam organisasi. Tag adalah pasangan key/value string yang dapat Anda gunakan untuk mengkategorikan dan memberi label sumber daya di akun Anda. Untuk informasi selengkapnya tentang penandaan, lihat Editor Tag di Panduan AWS Resource Groups Pengguna. Untuk informasi tentang menggunakan tag sebagai bagian dari strategi kontrol akses berbasis atribut, lihat Apa itu ABAC AWS di Panduan Pengguna IAM. Cuplikan contoh berikut membatasi kebijakan untuk diterapkan hanya pada akun di organisasi yang memiliki tag dengan kunci `project` dan nilai salah satu ataublue. `red`

Karena `account:AccountResourceOrgTags` merupakan tipe string multi-nilai, Anda harus menggunakan ForAnyValue atau operator string ForAllValues multi-nilai. Juga, perhatikan bahwa awalan pada kunci kondisi adalah`account`, meskipun Anda merujuk tag pada akun anggota organisasi.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgTags/project": [
            "blue",
            "red"
        ]
    }
```

```
}
```

> **Note**
>
> Anda dapat melampirkan tag hanya ke akun dalam organisasi. Anda tidak dapat melampirkan tag ke mandiri Akun AWS.

Konfigurasikan Anda Akun AWS

Petunjuk ini adalah tentang cara mengonfigurasi Akun AWS apakah Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Bagian ini mencakup topik yang menjelaskan cara mengelola Anda Akun AWS.

> **Note**
>
> Jika Anda Akun AWS dibuat di India menggunakan Amazon Web Services India Private Limited (AWS India), ada pertimbangan tambahan. Lihat informasi yang lebih lengkap di Kelola akun di India.

Topik

- Buat Akun AWS alias
- Aktifkan atau menonaktifkan Wilayah AWS di akun Anda
- Perbarui tagihan untuk Anda Akun AWS
- Perbarui alamat email pengguna root
- Perbarui kata sandi pengguna root
- Perbarui Anda Akun AWS name
- Perbarui kontak alternatif untuk Anda Akun AWS
- Perbarui kontak utama untuk Anda Akun AWS
- Tampilan Akun AWS pengidentifikasi

Buat Akun AWS alias

Petunjuk ini adalah tentang cara membuat Akun AWS alias jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Jika Anda ingin URL pengguna IAM berisi nama perusahaan Anda (atau pengenal lain yang mudah diingat) alih-alih Akun AWS ID, Anda dapat membuat alias akun.

Untuk mempelajari cara membuat atau memperbarui alias akun, lihat Menggunakan alias untuk Akun AWS ID Anda di Panduan Pengguna IAM.

Aktifkan atau menonaktifkan Wilayah AWS di akun Anda

Informasi ini adalah tentang mengaktifkan atau menonaktifkan Wilayah AWS Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

An Wilayah AWS adalah lokasi fisik di dunia yang AWS memiliki beberapa Zona Ketersediaan. Zona Ketersediaan terdiri dari satu atau lebih pusat AWS data terpisah, masing-masing dengan daya redundan, jaringan, dan konektivitas, ditempatkan di fasilitas terpisah. Ini berarti bahwa masing-masing Wilayah AWS secara fisik terisolasi dan independen dari Wilayah lainnya. Wilayah memberikan toleransi kesalahan, stabilitas, serta ketahanan, dan juga dapat mengurangi latensi. Menjalankan beban kerja Wilayah AWS lebih dekat dengan pengguna akhir dapat meningkatkan kinerja dan menurunkan latensi. Untuk peta Wilayah yang tersedia dan yang akan datang, lihat Wil ayah dan Zona Ketersediaan. Untuk mempelajari lebih lanjut tentang Wilayah AWS arsitektur ketahanan untuk beban kerja Anda, kunjungi Dasar-dasar AWS multi-wilayah.

Wilayah AWS secara luas jatuh ke dalam dua kategori ketersediaan untuk akun:

- Wilayah Def ault — Wilayah yang diluncurkan sebelum 20 Maret 2019 diaktifkan secara default. Anda dapat membuat dan mengelola sumber daya di Wilayah default ini segera setelah aktivasi akun Anda. Wilayah default tidak dapat diaktifkan atau dinonaktifkan.
- Opt-in Wilayah — Wilayah yang diluncurkan setelah 20 Maret 2019 dinonaktifkan secara default dan disebut sebagai Wilayah pilihan. Wilayah pilihan yang dinonaktifkan tidak ditampilkan di bilah Navigasi Konsol, dan Anda tidak dapat menggunakan Wilayah ini untuk membuat beban kerja sampai mereka diaktifkan. Untuk menggunakan Wilayah opt-in ini, Anda harus terlebih dahulu mengaktifkannya di wilayah Anda. Akun AWS Setelah mengaktifkan Wilayah pilihan, Anda dapat

memilih Wilayah tersebut di bilah navigasi dan membuat serta mengelola sumber daya di Wilayah tersebut. Untuk mengaktifkan Wilayah opt-in untuk akun mandiri Anda, lihat Mengaktifkan atau menonaktifkan Wilayah untuk akun mandiri dan untuk mengaktifkan Wilayah opt-in untuk akun anggota Anda, lihat. Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda

Saat Anda mendaftar Akun AWS, AWS merekomendasikan Wilayah pilihan untuk Anda berdasarkan negara alamat kontak Anda. Pelanggan di negara dengan Wil AWS ayah opt-in melihat rekomendasi di halaman Informasi Kontak untuk mengaktifkan Wilayah opt-in di negara tersebut. Pelanggan di negara dengan Wilayah opt-in dan Wilayah default, seperti India, Australia, atau Kanada, melihat rekomendasi untuk memilih Wilayah pilihan jika Wilayah opt-in lebih dekat dengan mereka daripada Wilayah default. Setelah akun diaktifkan, Anda dapat mengaktifkan Wilayah pilihan lain AWS di akun Anda atau memilih untuk menonaktifkan Wilayah opt-in yang Anda aktifkan saat mendaftar.

Saat Anda membuat Akun AWS, data dan kredenSIAL IAM Anda secara otomatis dikonfigurasi untuk bekerja di semua Wilayah default, memungkinkan pengguna root dan identitas IAM dengan izin yang sesuai untuk mengakses AWS layanan di Wilayah ini menggunakan kredensialnya yang ada. AWS Wilayah pilihan dinonaktifkan secara default, dan data serta kredenSIAL IAM pada awalnya tidak tersedia di Wilayah ini, yang mencegah akses ke AWS layanan di Wilayah tersebut. Saat Anda memilih untuk mengaktifkan Wilayah opt-in, menye AWS barkan data dan kredenSIAL IAM Anda ke Wilayah tersebut. Setelah propagasi selesai dan Wilayah opt-in diaktifkan, pengguna root dan identitas IAM kemudian dapat mengakses AWS layanan di Wilayah opt-in yang baru diaktifkan menggunakan kredentif IAM yang sama yang mereka gunakan di Wilayah default.

Saat Anda menonaktifkan Wilayah opt-in, kredentif IAM Anda dinonaktifkan dan Anda kehilangan akses IAM ke sumber daya di Wilayah pilihan tersebut. Menonaktifkan Wilayah pilihan tidak menghapus sumber daya di Wilayah tersebut dan biaya untuk sumber daya (jika ada) di Wilayah pilihan yang dinonaktifkan itu terus bertambah dengan tarif standar.

> **Important**
>
> Menonaktifkan Wilayah menonaktifkan akses IAM ke sumber daya di Wilayah. Ini tidak menghapus sumber daya yang dimaksud, yang terus dikenakan biaya. Hapus sumber daya yang tersisa sebelum menonaktifkan Wilayah.

AWS mengelompokkan Wilayah ke dalam partisi. Setiap wilayah berada tepat 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.

AWS Wilayah komersial berada di `aws` partisi, Wilayah di China berada di `aws-cn` partisi, dan AWS GovCloud (US) Wilayah berada di `aws-us-gov` partisi. Tergantung pada partisi tempat Anda membuat Akun AWS, Anda dapat menggunakannya di Wilayah AWS dalam partisi itu.

- Akun di `aws` partisi memberi Anda akses ke beberapa Wilayah di partisi komersial sehingga Anda dapat meluncurkan AWS sumber daya di lokasi yang memenuhi kebutuhan Anda. Misalnya, Anda mungkin ingin meluncurkan instans Amazon EC2 di Eropa agar lebih dekat dengan pelanggan Eropa Anda atau untuk memenuhi persyaratan hukum.
- Akun di `aws-us-gov` partisi memberi Anda akses ke AWS GovCloud (US-West) Region dan AWS GovCloud (US-East) Region. Untuk informasi selengkapnya, lihat AWS GovCloud (US).
- Akun di `aws-cn` partisi memberi Anda akses ke Wilayah Beijing dan Ningxia saja. Untuk informasi selengkapnya, lihat Amazon Web Services di Tiongkok.

Topik

- Referensi ketersediaan regional
- Pertimbangan Sebelum Mengaktifkan dan Menonaktifkan Wilayah
- Waktu pemrosesan dan batas permintaan
- Mengaktifkan atau menonaktifkan Wilayah untuk akun mandiri
- Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda

Referensi ketersediaan regional

Daftar tabel berikut Wilayah AWS berdasarkan jenis ketersediaan. Wilayah Default diaktifkan secara otomatis dan tidak dapat dinonaktifkan, sementara Wilayah pilihan harus diaktifkan secara manual sebelum Anda dapat menggunakannya:

Opt-in Regions

Wilayah berikut adalah Wilayah pilihan yang harus diaktifkan sebelum Anda dapat menggunakannya:

Nama	Kode	Status
Africa (Cape Town)	`af-south-1`	GA
Asia Pasifik (Hong Kong)	`ap-east-1`	GA

Nama	Kode	Status
Asia Pasifik (Taipei)	ap-east-2	GA
Asia Pasifik (Hyderabad)	ap-south-2	GA
Asia Pasifik (Jakarta)	ap-southeast-3	GA
Asia Pacific (Melbourne)	ap-southeast-4	GA
Asia Pasifik (Malaysia)	ap-southeast-5	GA
Asia Pasifik (Selandia Baru)	ap-southeast-6	GA
Asia Pasifik (Thailand)	ap-southeast-7	GA
Kanada Barat (Calgary)	ca-west-1	GA
Europe (Zurich)	eu-central-2	GA
Europe (Milan)	eu-south-1	GA
Eropa (Spanyol)	eu-south-2	GA
Israel (Tel Aviv)	il-central-1	GA
Timur Tengah (UAE)	me-central-1	GA
Timur Tengah (Bahrain)	me-south-1	GA
Meksiko (Tengah)	mx-central-1	GA

Default Regions

Wilayah berikut diaktifkan secara default dan tidak dapat dinonaktifkan:

Nama	Kode
Asia Pasifik (Tokyo)	ap-northeast-1

Nama	Kode
Asia Pasifik (Seoul)	`ap-northeast-2`
Asia Pasifik (Osaka)	`ap-northeast-3`
Asia Pasifik (Mumbai)	`ap-south-1`
Asia Pasifik (Singapura)	`ap-southeast-1`
Asia Pacific (Sydney)	`ap-southeast-2`
Kanada (Pusat)	`ca-central-1`
Eropa (Frankfurt)	`eu-central-1`
Eropa (Stockholm)	`eu-north-1`
Eropa (Irlandia)	`eu-west-1`
Eropa (London)	`eu-west-2`
Eropa (Paris)	`eu-west-3`
Amerika Selatan (São Paulo)	`sa-east-1`
AS Timur (Virginia Utara)	`us-east-1`
AS Timur (Ohio)	`us-east-2`
AS Barat (California Utara)	`us-west-1`
AS Barat (Oregon)	`us-west-2`

Untuk daftar nama Wilayah dan kode yang sesuai, lihat Titik akhir Regional di Panduan Refer AWS ensi Umum. Untuk daftar AWS layanan yang didukung di setiap Wilayah (tanpa titik akhir), lihat Daftar Layanan AWS Regional.

> **Important**
>
> AWS merekomendasikan agar Anda menggunakan titik akhir regional AWS Security Token Service (AWS STS) alih-alih titik akhir global untuk mengurangi latensi. Token sesi dari AWS STS titik akhir regional berlaku di semua Wil AWS ayah. Jika Anda menggunakan AWS STS titik akhir regional, Anda tidak perlu membuat perubahan apa pun. Namun, token sesi dari AWS STS titik akhir global (https://sts.amazonaws.com) hanya valid jika Wilayah AWS Anda mengaktifkan, atau yang diaktifkan secara default. Jika Anda ingin mengaktifkan Wilayah baru untuk akun Anda, Anda dapat menggunakan token sesi dari titik akhir AWS STS regional atau mengaktifkan titik AWS STS akhir global untuk mengeluarkan token sesi yang valid di semua Wilayah AWS. Token sesi yang valid di semua Wilayah memiliki ukuran yang lebih besar. Jika Anda menyimpan token sesi, token yang lebih besar ini dapat memengaruhi sistem Anda. Untuk informasi selengkapnya tentang cara AWS STS kerja titik akhir dengan Wil AWS ayah, lihat M engelola AWS STS di Wil AWS ayah.

Pertimbangan Sebelum Mengaktifkan dan Menonaktifkan Wilayah

Sebelum Anda mengaktifkan atau menonaktifkan Wilayah, penting untuk mempertimbangkan hal-hal berikut:

- Anda dapat menggunakan semua Wilayah tujuan dalam geografi inferensi lintas wilayah terlepas dari Region-opt statusnya — Layanan AI AWS generatif tertentu termasuk Amazon Bedrock (lihat Mening katkan throughput dengan inferensi lintas wilayah) dan Amazon Q Developer (lihat Cross-region pemrosesan di Amazon Q Developer) menggunakan inferensi lintas wilayah. Jika Anda menggunakan layanan tersebut, layanan tersebut secara otomatis memilih yang optimal Wilayah AWS— termasuk Wilayah yang belum Anda aktifkan untuk sumber daya dan data IAM — dalam geografi yang Anda pilih. Ini meningkatkan pengalaman pelanggan dengan memaksimalkan ketersediaan komputasi dan model yang tersedia.
- Anda dapat menggunakan izin IAM untuk mengontrol akses ke Wilayah — AWS Identity and Access Management (IAM) mencakup empat izin yang memungkinkan Anda mengontrol pengguna mana yang dapat mengaktifkan, menonaktifkan, mendapatkan, dan membuat daftar Wilayah. Untuk informasi selengkapnya, lihat AWS: Memungkinkan mengaktifkan dan menonaktifkan Wilayah AWS di Panduan Pengguna IAM. Anda juga dapat menggunakan kunci `aws:RequestedRegion` kondisi untuk mengontrol akses ke Layanan AWS dalam Wilayah AWS.

- Mengaktifkan dan menonaktifkan Wilayah gratis — Tidak ada biaya untuk mengaktifkan atau menonaktifkan Wilayah. Anda hanya dikenakan biaya untuk sumber daya yang Anda buat di Wilayah baru.
- EventBridge Integrasi Amazon — Anda dapat berlangganan pemberitahuan pembaruan status region-opt di. EventBridge Pem EventBridge beritahuan akan dibuat untuk setiap perubahan status, memungkinkan pelanggan untuk mengotomatiskan alur kerja.
- Region-opt Status ekspresif — Karena sifat asinkron dari enabling/disabling wilayah opt-in, ada empat status potensial untuk permintaan region-opt:
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  Anda tidak dapat membatalkan opt-in atau opt-out saat berada dalam salah satu `ENABLING` atau `DISABLING` status. Kalau tidak, wasiat `ConflictException` akan dilemparkan. Permintaan region-opt yang telah selesai (Enabled/Disabled) bergantung pada penyediaan layanan utama yang mendasarinya. AWS Mungkin ada beberapa AWS layanan yang tidak akan segera dapat digunakan meskipun statusnya ada`ENABLED`.

Waktu pemrosesan dan batas permintaan

Saat mengaktifkan atau menonaktifkan Wilayah, perhatikan batasan waktu dan permintaan berikut:

- Mengaktifkan Wilayah membutuhkan waktu beberapa menit hingga beberapa jam dalam beberapa kasus — Saat Anda mengaktifkan Wilayah, lakukan AWS tindakan untuk mempersiapkan akun Anda di Wilayah tersebut, seperti mendistribusikan sumber daya IAM Anda ke Wilayah. Proses ini memakan waktu beberapa menit untuk sebagian besar akun, tetapi terkadang dapat memakan waktu beberapa jam. Anda tidak dapat menggunakan Wilayah sampai proses ini selesai.
- Menonaktifkan Wilayah tidak selalu langsung terlihat — Layanan dan konsol mungkin terlihat sementara setelah menonaktifkan wilayah. Menonaktifkan Wilayah dapat memakan waktu beberapa menit hingga beberapa jam untuk berlaku.
- Satu akun dapat memiliki 6 permintaan pilihan wilayah yang sedang berlangsung pada waktu tertentu — Satu permintaan sama dengan mengaktifkan atau menonaktifkan satu wilayah tertentu untuk satu akun.

- Organisasi dapat membuka 50 permintaan pilihan wilayah pada waktu tertentu di seluruh AWS organisasi — Akun manajemen dapat setiap saat memiliki 50 permintaan terbuka yang menunggu penyelesaian untuk organisasinya. Satu permintaan sama dengan mengaktifkan atau menonaktifkan satu wilayah tertentu untuk satu akun.

Mengaktifkan atau menonaktifkan Wilayah untuk akun mandiri

Untuk memperbarui Wilayah mana yang dapat Anda Akun AWS akses, lakukan langkah-langkah dalam prosedur berikut. Konsol Manajemen AWS Prosedur berikut selalu bekerja hanya dalam konteks mandiri. Anda dapat menggunakan Konsol Manajemen AWS untuk melihat atau memperbarui hanya Wilayah yang tersedia di akun yang Anda gunakan untuk memanggil operasi.

Konsol Manajemen AWS

Untuk mengaktifkan atau menonaktifkan Wilayah untuk mandiri Akun AWS

> **Izin minimum**
>
> Untuk melakukan langkah-langkah dalam prosedur berikut, pengguna atau peran IAM harus memiliki izin berikut:
>
> - `account:ListRegions`(diperlukan untuk melihat daftar Wilayah AWS dan apakah mereka saat ini diaktifkan atau dinonaktifkan).
> - `account:EnableRegion`
> - `account:DisableRegion`

1. Masuk ke Konsol Manajemen AWS sebagai Pengguna root akun AWS atau sebagai pengguna atau peran IAM yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Pada halaman Akun, gulir ke bawah ke bagian Wilayah AWS.
4. Pilih Wilayah yang ingin Anda aktifkan atau nonaktifkan lalu pilih tindakan yang diinginkan Aktifkan atau Non aktifkan. Anda akan melihat prompt untuk mengonfirmasi.
5. Jika Anda memilih opsi Aktifkan, tinjau teks yang ditampilkan, lalu pilih Aktifkan wilayah.

   Jika Anda memilih opsi N onaktifkan, tinjau teks yang ditampilkan, ketik **`disable`** untuk mengonfirmasi, lalu pilih N onaktifkan wilayah.

Setelah Wilayah opt-in diaktifkan, Anda dapat memilih Wilayah tersebut dari bilah navigasi Wilayah. Untuk langkah-langkah memilih Wilayah, lihat Memilih Wilayah dari bilah navigasi di Konsol Manajemen AWS dan untuk pengaturan konsol khusus Wilayah di akun Anda, lihat Mengatur Wilayah default di Konsol Manajemen AWS.

AWS CLI & SDKs

Anda dapat mengaktifkan, menonaktifkan, membaca, dan mencantumkan status pilihan wilayah dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki izin yang dipetakan ke operasi itu:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca informasi pilihan wilayah, dan memberi orang lain kemampuan untuk membaca dan menulis.

Contoh berikut mengaktifkan wilayah untuk akun anggota tertentu dalam organisasi. KredenSIAL yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

Perhatikan bahwa Anda juga dapat menonaktifkan wilayah menggunakan perintah yang sama dan kemudian mengganti `enable-region` dengan`disable-region`.

```
aws account enable-region --region-name af-south-1
```

Perintah ini tidak menghasilkan output jika berhasil.

Operasi ini asinkron. Perintah berikut akan memungkinkan Anda untuk melihat status permintaan terbaru.

```
aws account get-region-opt-status --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda

Untuk memperbarui Wilayah yang diaktifkan untuk akun anggota Anda AWS Organizations, lakukan langkah-langkah dalam prosedur berikut.

> **Note**
>
> Kebijakan AWS Organizations terkelola `AWSOrganizationsReadOnlyAccess` atau `AWSOrganizationsFullAccess` diperbarui untuk memberikan izin untuk mengakses API Manajemen AWS Akun sehingga Anda dapat mengakses data akun dari AWS Organizations konsol. Untuk melihat kebijakan terkelola yang diperbarui, lihat Pembaruan kebijakan yang AWS dikelola Organisasi.

> **Note**
>
> Sebelum Anda dapat melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan dalam organisasi untuk digunakan dengan akun anggota, Anda harus:
>
> - Aktifkan semua fitur di organisasi Anda untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi Anda. Jika organisasi Anda disetel ke tagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat Mengaktifkan semua fitur di organisasi Anda.

- Aktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihatAktifkan akses tepercaya untuk AWS Pengelolaan Akun.

Konsol Manajemen AWS

Untuk mengaktifkan atau menonaktifkan Wilayah di organisasi Anda

1. Masuk ke AWS Organizations konsol dengan kredenSIAL akun manajemen organisasi Anda.
2. Pada Akun AWS halaman, pilih akun yang ingin Anda perbarui.
3. Pilih tab Pengaturan akun.
4. Di bawah Wilayah, pilih Wilayah yang ingin Anda aktifkan atau nonaktifkan.
5. Pilih T ind akan, lalu pilih opsi Aktifkan atau Nonaktifkan.
6. Jika Anda memilih opsi Aktifkan, tinjau teks yang ditampilkan, lalu pilih Aktifkan wilayah.
7. Jika Anda memilih opsi N onaktifkan, tinjau teks yang ditampilkan, ketik nonaktifkan untuk mengonfirmasi, lalu pilih N onaktifkan wilayah.

AWS CLI & SDKs

Anda dapat mengaktifkan, menonaktifkan, membaca, dan mencantumkan status pilihan wilayah untuk akun anggota organisasi dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki izin yang dipetakan ke operasi itu:

- `account:EnableRegion`
- `account:DisableRegion`

- `account:GetRegionOptStatus`
- `account:ListRegions`

Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca informasi pilihan wilayah, dan memberi orang lain kemampuan untuk membaca dan menulis.

Contoh berikut mengaktifkan wilayah untuk akun anggota tertentu dalam organisasi. KredenSIAL yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

Perhatikan bahwa Anda juga dapat menonaktifkan wilayah menggunakan perintah yang sama dan kemudian mengganti `enable-region` dengan`disable-region`.

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

Perintah ini tidak menghasilkan output jika berhasil.

> **Note**
>
> Sebuah organisasi hanya dapat memiliki hingga 20 permintaan wilayah pada waktu tertentu. Jika tidak, Anda akan menerima a`TooManyRequestsException`.

Operasi ini asinkron. Perintah berikut akan memungkinkan Anda untuk melihat status permintaan terbaru.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Perbarui tagihan untuk Anda Akun AWS

Petunjuk ini adalah tentang cara memperbarui penagihan Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Anda dapat memperbarui semua preferensi Akun AWS penagihan menggunakan konsol Manajemen Biaya. AWS Billing Untuk mempelajari cara memperbarui setelan terkait penagihan untuk akun Anda, lihat Panduan AWS Manajemen Penagihan dan Biaya Pengguna:

Perbarui alamat email pengguna root

Petunjuk ini adalah untuk cara memperbarui alamat email pengguna root jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Ada berbagai alasan bisnis mengapa Anda mungkin perlu memperbarui alamat email pengguna root Anda Akun AWS. Misalnya, keamanan dan ketahanan administratif. Topik ini memandu Anda melalui proses memperbarui alamat email pengguna root Anda alamat email untuk akun mandiri dan akun anggota.

> **Note**
>
> Perubahan pada an Akun AWS bisa memakan waktu hingga empat jam untuk menyebar ke mana-mana.

Anda dapat memperbarui email pengguna root email secara berbeda, tergantung pada apakah akun berdiri sendiri atau tidak, atau bagian dari organisasi:

- Akun mandiri Akun AWS atau manajemen — Untuk Akun AWS tidak terkait dengan organisasi, atau untuk akun manajemen organisasi, Anda dapat memperbarui email pengguna root menggunakan Konsol AWS Manajemen. Untuk mempelajari cara melakukannya, lihat Memperbarui email pengguna root email untuk akun mandiri Akun AWS atau manajemen.
- Akun AWS dalam organisasi — Untuk akun anggota yang merupakan bagian dari AWS organisasi, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui email pengguna root email dari akun anggota dari AWS Organizations konsol, atau secara terprogram melalui CLI AWS & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui email pengguna root untuk semua orang Akun AWS di organisasi Anda.

Topik

- Perbarui email pengguna root untuk standalone Akun AWS atau akun manajemen
- Perbarui email pengguna root untuk setiap Akun AWS di organisasi Anda

Perbarui email pengguna root untuk standalone Akun AWS atau akun manajemen

Untuk mengedit alamat email pengguna root alamat untuk akun mandiri Akun AWS atau akun manajemen, lakukan langkah-langkah dalam prosedur berikut.

Konsol Manajemen AWS

> **Note**
>
> Anda harus masuk sebagai Pengguna root akun AWS, yang tidak memerlukan izin IAM tambahan. Anda tidak dapat melakukan langkah-langkah ini sebagai pengguna atau peran IAM.

1. Gunakan alamat email dan kata sandi Anda untuk masuk ke Konsol Manajemen AWSsebagai Akun AWS milik Anda Pengguna root akun AWS.
2. Di sudut kanan atas konsol, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada halaman Akun, di samping Detail akun, pilih Tindakan, lalu pilih Perbarui alamat email dan kata sandi.
4. Pada halaman Detail Akun, di samping Alamat email pilih Edit.
5. Pada halaman Edit Email Akun, isi kolom untuk Alamat email baru, Konfirmasikan alamat email baru, dan konfirmasikan Kata Sandi Anda saat ini. Kemudian, pilih Simpan dan lanjutkan. Kode verifikasi dikirim ke alamat email baru Anda dari`no-reply@verify.signin.aws`.
6. Pada halaman Edit Email Akun, di bawah kode Verifikasi, masukkan kode yang Anda terima dari email Anda, lalu pilih Konfirmasi pembaruan.

> **Note**
>
> Diperlukan waktu hingga 5 menit agar kode verifikasi tiba. Jika Anda tidak melihat email di kotak masuk Anda, periksa folder spam dan sampah Anda.

AWS CLI & SDKs

Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

Perbarui email pengguna root untuk setiap Akun AWS di organisasi Anda

Untuk mengedit alamat email pengguna root alamat untuk setiap akun anggota di organisasi Anda menggunakan AWS Organizations konsol, lakukan langkah-langkah dalam prosedur berikut.

> **Note**
>
> Sebelum Anda memperbarui alamat email pengguna root alamat untuk akun anggota, kami sarankan Anda memahami dampak dari operasi ini. Untuk informasi selengkapnya, lihat Memperbarui alamat email pengguna root untuk akun anggota AWS Organizations di Panduan AWS Organizations Pengguna.

Anda juga dapat memperbarui alamat email pengguna root alamat untuk akun anggota langsung dari halaman Akun Konsol Manajemen AWS setelah masuk sebagai pengguna root. Untuk petunjuk langkah demi langkah, ikuti langkah-langkah yang disediakan diPerbarui email pengguna root untuk standalone Akun AWS atau akun manajemen.

> **Note**
>
> Anda tidak dapat memperbarui alamat email pengguna root dari akun proyek, yang merupakan akun anggota yang Anda buat sebagai proyek di AWS Pengaturan. ID AWS Builder memiliki setiap akun proyek, bukan alamat email pengguna root, dan ini tidak berubah saat Anda mengaktifkan fitur lanjutan. Untuk informasi selengkapnya, lihat Akun proyek setelah Anda mengaktifkan fitur lanjutan.

AWS Management Console

> **Catatan**
>
> - Untuk melakukan prosedur ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun.
> - Anda tidak dapat menggunakan prosedur ini untuk mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

Untuk memperbarui alamat email pengguna root untuk akun anggota menggunakan AWS Organizations konsol

1. Masuk ke konsol AWS Organizations tersebut. Anda harus masuk sebagai pengguna IAM, atau masuk sebagai pengguna root (tidak disarankan) di akun manajemen organisasi.
2. Pada Akun AWShalaman, pilih akun anggota yang ingin Anda perbarui alamat email pengguna root alamat email .
3. Di bagian Detail akun, pilih tombol Tindakan, lalu pilih Perbarui alamat email.
4. Di bawah Email, masukkan alamat email baru untuk pengguna root, lalu pilih Simpan. Ini mengirimkan kata sandi satu kali (OTP) ke alamat email baru.

   > **Note**
   >
   > Jika Anda perlu menutup halaman ini di konsol Organizations sambil menunggu kode, Anda dapat mengembalikan dan menyelesaikan proses OTP dalam waktu 24 jam sejak kode dikirim. Untuk melakukan ini, saat berada di halaman Detail akun, pilih tombol Tindakan, lalu pilih Selesaikan pembaruan email.

5. Di bawah Kode verifikasi, masukkan kode yang dikirim ke alamat email baru pada langkah sebelumnya, lalu pilih Konfirmasi. Ini melakukan pembaruan ke pengguna root untuk akun tersebut.

AWS CLI & SDKs

Anda dapat mengambil, atau memperbarui alamat email pengguna root (juga disebut sebagai alamat email utama) dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

> **Catatan**
>
> - Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun.
> - Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.
> - Untuk akun proyek, `StartPrimaryEmailUpdate` dan `AcceptPrimaryEmailUpdate` gagal dengan `AccessDeniedException` kesalahan bahkan ketika Anda memiliki izin yang diperlukan.

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:
>
> - `account:GetPrimaryEmail`
> - `account:StartPrimaryEmailUpdate`
> - `account:AcceptPrimaryEmailUpdate`
>
> Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca alamat email pengguna root informasi alamat email , dan memberi orang lain kemampuan untuk membaca dan menulis.

Untuk menyelesaikan proses alamat email pengguna root, Anda harus menggunakan API email utama bersama-sama dalam urutan yang ditampilkan dalam contoh berikut.

Example **`GetPrimaryEmail`**

Contoh berikut mengambil alamat email pengguna root alamat email dari akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account get-primary-email --account-id 123456789012
```

Example **`StartPrimaryEmailUpdate`**

Contoh berikut memulai proses pembaruan alamat email pengguna root baru, dan mengirimkan kata sandi satu kali (OTP) ke alamat email baru untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email
 john@examplecorp.com
```

Example **`AcceptPrimaryEmailUpdate`**

Contoh berikut menerima kode OTP dan menetapkan alamat email baru ke akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

Perbarui kata sandi pengguna root

Petunjuk ini adalah tentang cara memperbarui kata sandi pengguna root jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Untuk mengedit Akun AWS kata sandi pengguna root Anda, lakukan langkah-langkah dalam prosedur berikut.

Konsol Manajemen AWS

Untuk mengedit kata sandi pengguna root Anda

> **Note**
>
> Anda harus masuk sebagai Pengguna root akun AWS, yang tidak memerlukan izin IAM tambahan. Anda tidak dapat melakukan langkah-langkah ini sebagai pengguna atau peran IAM.

1. Gunakan Akun AWS alamat email dan kata sandi Anda untuk masuk Konsol Manajemen AWS sebagai milik Anda Pengguna root akun AWS.
2. Di sudut kanan atas konsol, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada halaman Akun, di samping Detail akun, pilih Tind akan lalu pilih Per barui alamat email dan kata sandi.
4. Pada halaman Detail Akun, di samping Kata Sand i pilih Edit.
5. Pada halaman Edit kata sandi, isi kolom untuk Kata sandi saat ini, Kata sandi baru, dan Kon firmasi kata sandi baru. Kemudian, pilih Per barui kata sandi. Untuk panduan tambahan termasuk praktik terbaik untuk menyetel kata sandi pengguna root, lihat Meng ubah kata sandi untuk Pengguna root akun AWS di Panduan Pengguna IAM.

AWS CLI & SDKs

Tugas ini tidak didukung dalam AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

Perbarui Anda Akun AWS name

Petunjuk ini adalah tentang cara memperbarui Akun AWS nama Anda jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Saat mengelola banyak Akun AWS, gunakan konvensi penamaan yang jelas yang selaras dengan unit bisnis dan aplikasi untuk identifikasi dan organisasi. Selama reorganisasi, merger, akuisisi, atau pembaruan konvensi penamaan, Anda mungkin perlu mengganti nama akun untuk mempertahankan identifikasi dan standar administrasi yang konsisten.

Nama akun muncul di beberapa tempat, seperti pada faktur Anda dan di konsol seperti dasbor Penagihan dan Manajemen Biaya dan AWS Organizations konsol. Kami menyarankan Anda menggunakan cara standar untuk memberi nama akun Anda sehingga nama akun Anda mudah dikenali. Untuk akun perusahaan, pertimbangkan untuk menggunakan standar penamaan seperti organisasi - tujuan - lingkungan (misalnya, penjualan - katalog - produk). Untuk alasan privasi dan keamanan, hindari menggunakan nama akun yang mencerminkan informasi identitas pribadi (PII).

- Akun mandiri Akun AWS atau manajemen — Untuk Akun AWS tidak terkait dengan organisasi, atau untuk akun manajemen organisasi, Anda dapat memperbarui nama akun menggunakan Konsol Manajemen AWS, atau AWS CLI dan SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui nama akun Anda untuk mandiri Akun AWS atau akun manajemen.
- Akun AWS dalam organisasi — Untuk akun anggota yang merupakan bagian dari AWS Organizations, pengguna di akun manajemen atau akun admin yang didelegasikan dapat secara terpusat memperbarui nama akun anggota mana pun di organisasi dari AWS Organizations konsol, atau secara terprogram melalui SDK AWS CLI and. Untuk mempelajari cara melakukannya, lihat Perbarui nama akun Anda untuk semua Akun AWS dalam organisasi Anda.

> **Note**
>
> Perubahan kal Akun AWS eng membutuhkan waktu hingga empat jam untuk menyebar di mana-mana.

Topik

- Memperbarui nama akun Anda untuk mandiri Akun AWS atau akun manajemen
- Perbarui nama akun Anda untuk semua Akun AWS dalam organisasi Anda

Memperbarui nama akun Anda untuk mandiri Akun AWS atau akun manajemen

Untuk mengubah nama akun untuk akun mandiri Akun AWS atau manajemen, lakukan langkah-langkah dalam prosedur berikut.

Konsol Manajemen AWS

> **Izin minimum**
>
> Anda dapat memperbarui nama akun menggunakan pengguna root, pengguna IAM, atau peran IAM. Jika Anda menggunakan pengguna root, tidak diperlukan izin IAM tambahan untuk memperbarui nama akun. Saat menggunakan pengguna IAM atau peran IAM, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Untuk memperbarui nama akun untuk akun mandiri atau akun manajemen

1. Gunakan Akun AWS alamat email dan kata sandi Anda untuk masuk Konsol Manajemen AWS sebagai milik Anda Pengguna root akun AWS.
2. Di sudut kanan atas konsol, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada halaman Akun, di samping Detail akun, pilih Tind akan lalu pilih Per barui nama akun.
4. Di bawah Nama, masukkan nama akun baru yang ingin Anda perbarui, lalu pilih S impan.

AWS CLI & SDKs

> **Izin minimum**
>
> Anda dapat memperbarui nama akun menggunakan pengguna root, pengguna IAM, atau peran IAM. Untuk melakukan langkah-langkah berikut, pengguna IAM atau peran IAM Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Untuk memperbarui nama akun untuk akun mandiri atau akun manajemen

Anda dapat menggunakan salah satu operasi berikut:

- AWS CLI: masukkan nam a-akun

```
$ C:\> aws account put-account-name \
        --account-name "New-Account-Name"
```

- AWS SDK: PutAccountName

Perbarui nama akun Anda untuk semua Akun AWS dalam organisasi Anda

Dalam AWS Organizations mode semua fitur, pengguna IAM resmi atau peran IAM di manajemen dan akun admin yang didelegasikan dapat mengelola nama akun secara terpusat.

Untuk mengubah nama akun untuk setiap akun anggota di organisasi Anda, lakukan langkah-langkah dalam prosedur berikut.

Persyaratan

Untuk memperbarui nama akun dengan AWS Organizations konsol, Anda perlu melakukan beberapa pengaturan awal:

- Organisasi Anda harus mengaktifkan semua fitur untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi Anda. Jika organisasi Anda disetel ke tagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat Mengaktifkan semua fitur untuk organisasi.
- Anda perlu mengaktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihatAktifkan akses tepercaya untuk AWS Pengelolaan Akun.

Konsol Manajemen AWS

> **Izin minimum**
>
> Untuk memperbarui nama akun untuk akun anggota, pengguna IAM atau peran IAM Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganization` (hanya konsol)
> - `account:PutAccountName`

Untuk memperbarui nama akun untuk akun anggota

1. Buka konsol Organisasi di https://console.aws.amazon.com/organizations/.
2. Di panel navigasi utama, pilih Akun AWS.
3. Pada Akun AWS halaman, pilih akun anggota yang ingin Anda perbarui, pilih menu tarik-turun Tindakan, lalu pilih Per barui nama akun.
4. Di bawah Nama, masukkan nama yang diperbarui, dan pilih S impan.

AWS CLI & SDKs

> **Izin minimum**
>
> Untuk memperbarui nama akun untuk akun anggota, pengguna IAM atau peran IAM Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganization` (hanya konsol)
> - `account:PutAccountName`

Untuk memperbarui nama akun untuk akun anggota

Anda dapat menggunakan salah satu operasi berikut:

- AWS CLI: masukkan nam a-akun

```
$ C:\> aws account put-account-name \
        --account-id 111111111111 \
        --account-name "New-Account-Name"
```

- AWS SDK: PutAccountName

Perbarui kontak alternatif untuk Anda Akun AWS

Petunjuk ini adalah tentang cara memperbarui kontak alternatif untuk Anda Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Kontak alternatif memungkinkan AWS untuk menghubungi hingga tiga kontak alternatif yang terkait dengan akun. Kontak alternatif tidak harus orang tertentu. Sebagai gantinya, Anda dapat menambahkan daftar distribusi email jika Anda memiliki tim yang mengelola masalah terkait penagihan, operasi, dan keamanan. Ini adalah tambahan ke alamat email yang terkait dengan pengguna ??? root akun. Kon tak akun utama akan terus menerima semua komunikasi email yang dikirim ke email akun root.

Anda hanya dapat menentukan satu dari masing-masing jenis kontak berikut yang terkait dengan akun.

- Kontak penagihan
- Kontak operasi
- Kontak keamanan

Anda dapat menambahkan atau mengedit kontak alternatif secara berbeda, tergantung pada apakah akun tersebut mandiri atau tidak, atau bagian dari organisasi:

- Man Akun AWS diri — Untuk Akun AWS tidak terkait dengan organisasi, Anda dapat memperbarui kontak alternatif Anda sendiri menggunakan Konsol AWS Manajemen, atau melalui AWS CLI & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui kontak alternatif untuk mandiri Akun AWS.
- Akun AWS dalam organisasi — Untuk akun anggota yang merupakan bagian dari AWS organisasi, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui akun anggota di organisasi secara terpusat dari AWS Organizations konsol, atau secara terprogram melalui AWS CLI & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui kontak alternatif untuk setiap kontak Akun AWS di organisasi Anda.

Topik

- Persyaratan nomor telepon dan alamat email
- Perbarui kontak alternatif untuk mandiri Akun AWS
- Perbarui kontak alternatif untuk apa pun Akun AWS dalam organisasi Anda
- account: kunci AlternateContactTypes konteks

Persyaratan nomor telepon dan alamat email

Sebelum Anda melanjutkan dengan memperbarui informasi kontak alternatif akun Anda, sebaiknya tinjau terlebih dahulu persyaratan berikut saat memasukkan nomor telepon dan alamat email.

- Nomor telepon hanya dapat berisi angka, spasi putih dan karakter berikut:"". `+-()`
- Alamat email dapat memiliki panjang hingga 254 karakter dan dapat menyertakan karakter khusus berikut di bagian lokal alamat email selain yang alfanumerik standar: "`+=.#|!&-_`".

Perbarui kontak alternatif untuk mandiri Akun AWS

Untuk menambah atau mengedit kontak alternatif untuk mandiri Akun AWS, lakukan langkah-langkah dalam prosedur berikut. Konsol Manajemen AWS Prosedur berikut selalu bekerja hanya dalam konteks mandiri. Anda dapat menggunakan Konsol Manajemen AWS untuk mengakses atau mengubah hanya kontak alternatif di akun yang Anda gunakan untuk memanggil operasi.

Konsol Manajemen AWS

Untuk menambah atau mengedit kontak alternatif untuk mandiri Akun AWS

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetAlternateContact`(untuk melihat detail kontak alternatif)
> - `account:PutAlternateContact`(untuk mengatur atau memperbarui kontak alternatif)
> - `account:DeleteAlternateContact`(untuk menghapus kontak alternatif)

1. Masuk ke Konsol Manajemen AWS sebagai pengguna atau peran IAM yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.

3. Pada halaman Akun, gulir ke bawah ke Kon tak alternatif, dan di sebelah kanan judul, pilih Edit.

> **Note**
>
> Jika Anda tidak melihat opsi Edit, kemungkinan Anda tidak masuk sebagai pengguna root untuk akun Anda atau sebagai seseorang yang memiliki izin minimum yang ditentukan sebelumnya.

4. Ubah nilai di salah satu bidang yang tersedia.

> **Important**
>
> Untuk bisnis Akun AWS, ini adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada milik individu.

5. Setelah Anda membuat semua perubahan, pilih Per barui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak alternatif dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Catatan**
>
> - Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan dalam organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Akun.

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:

- `GetAlternateContact`(untuk melihat detail kontak alternatif)
- `PutAlternateContact`(untuk mengatur atau memperbarui kontak alternatif)
- `DeleteAlternateContact`(untuk menghapus kontak alternatif)

Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil kontak alternatif Penagihan saat ini untuk akun penelepon.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

Contoh berikut menetapkan kontak alternatif Operasi baru untuk akun penelepon.

```
$ aws account put-alternate-contact \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Perintah ini tidak menghasilkan output jika berhasil.

Example

> **Note**
>
> Jika Anda melakukan beberapa `PutAlternateContact` operasi pada jenis kontak yang sama Akun AWS dan sama, yang pertama menambahkan kontak baru, dan semua panggilan berturut-turut ke jenis kontak yang sama Akun AWS dan kontak memperbarui kontak yang ada.

Example

Contoh berikut menghapus kontak alternatif Keamanan untuk akun penelepon.

```
$ aws account delete-alternate-contact \
    --alternate-contact-type=SECURITY
```

Perintah ini tidak menghasilkan output jika berhasil.

> **Note**
>
> Jika Anda mencoba menghapus kontak yang sama lebih dari sekali, yang pertama berhasil secara diam-diam. Semua upaya selanjutnya menghasilkan peng `ResourceNotFound` ecualian.

Perbarui kontak alternatif untuk apa pun Akun AWS dalam organisasi Anda

Untuk menambah atau mengedit detail kontak alternatif untuk setiap orang Akun AWS di organisasi Anda, lakukan langkah-langkah dalam prosedur berikut.

Persyaratan

Untuk memperbarui kontak alternatif dengan AWS Organizations konsol, Anda perlu melakukan beberapa pengaturan awal:

- Organisasi Anda harus mengaktifkan semua fitur untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi Anda. Jika organisasi Anda disetel ke tagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat Mengaktifkan semua fitur untuk organisasi.

- Anda perlu mengaktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihatAktifkan akses tepercaya untuk AWS Pengelolaan Akun.

> **Note**
>
> Kebijakan AWS Organizations terkelola `AWSOrganizationsReadOnlyAccess` atau `AWSOrganizationsFullAccess` diperbarui untuk memberikan izin untuk mengakses API Manajemen AWS Akun sehingga Anda dapat mengakses data akun dari AWS Organizations konsol. Untuk melihat kebijakan terkelola yang diperbarui, lihat Pembaruan kebijakan yang AWS dikelola Organisasi.

Konsol Manajemen AWS

Untuk menambah atau mengedit kontak alternatif untuk setiap Akun AWS dalam organisasi Anda

1. Masuk ke AWS Organizations konsol dengan kredenSIAL akun manajemen organisasi.
2. Dari Akun AWS, pilih akun yang ingin Anda perbarui.
3. Pilih Info kontak, dan di bawah Kontak alternatif, cari jenis kontak: Kontak penagihan, Kon tak keamanan, atau Kon tak operasi.
4. Untuk menambahkan kontak baru, pilih Tam bah, atau untuk memperbarui kontak yang sudah ada pilih Edit.
5. Ubah nilai di salah satu bidang yang tersedia.

   > **Important**
   >
   > Untuk bisnis Akun AWS, ini adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada milik individu.

6. Setelah Anda membuat semua perubahan, pilih Per barui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak alternatif dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetAlternateContact

- PutAlternateContact
- DeleteAlternateContact

> **Catatan**
>
> - Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan dalam organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Akun.
> - Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:
>
> - `GetAlternateContact`(untuk melihat detail kontak alternatif)
> - `PutAlternateContact`(untuk mengatur atau memperbarui kontak alternatif)
> - `DeleteAlternateContact`(untuk menghapus kontak alternatif)
>
> Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil kontak alternatif Penagihan saat ini untuk akun penelepon di organisasi. KredenSIAL yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING \
    --account-id 123456789012
```

```
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

Contoh berikut menetapkan kontak alternatif Operasi untuk akun anggota tertentu dalam organisasi. KredenSIAL yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Perintah ini tidak menghasilkan output jika berhasil.

> **Note**
>
> Jika Anda melakukan beberapa `PutAlternateContact` operasi pada jenis kontak yang sama Akun AWS dan sama, yang pertama menambahkan kontak baru, dan semua panggilan berturut-turut ke jenis kontak yang sama Akun AWS dan kontak memperbarui kontak yang ada.

Example

Contoh berikut menghapus kontak alternatif Keamanan untuk akun anggota tertentu di organisasi. KredenSIAL yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account delete-alternate-contact \
```

```
    --account-id 123456789012 \
    --alternate-contact-type=SECURITY
```

Perintah ini tidak menghasilkan output jika berhasil.

Example

> **Note**
>
> Jika Anda mencoba menghapus kontak yang sama lebih dari sekali, yang pertama berhasil secara diam-diam. Semua upaya selanjutnya menghasilkan peng `ResourceNotFound` ecualian.

account: kunci AlternateContactTypes konteks

Anda dapat menggunakan kunci konteks `account:AlternateContactTypes` untuk menentukan mana dari tiga jenis kontak yang diizinkan (atau ditolak) oleh kebijakan IAM. Misalnya, contoh kebijakan izin IAM berikut menggunakan kunci kondisi ini untuk mengizinkan prinsipal terlampir mengambil, tetapi tidak memodifikasi, hanya kontak `BILLING` alternatif untuk akun tertentu dalam organisasi.

Karena `account:AlternateContactTypes` merupakan tipe string multi-nilai, Anda harus menggunakan `ForAnyValue` atau operator string `ForAllValues` multi-nilai.

Perbarui kontak utama untuk Anda Akun AWS

Petunjuk ini adalah tentang cara memperbarui kontak utama untuk Anda Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Anda dapat memperbarui informasi kontak utama yang terkait dengan akun Anda, termasuk nama lengkap kontak Anda, nama perusahaan, alamat surat, nomor telepon, dan alamat situs web.

Anda juga dapat memverifikasi nomor telepon kontak utama. Untuk informasi selengkapnya, lihat Verifikasi nomor telepon kontak utama.

Anda mengedit kontak akun utama secara berbeda, tergantung pada apakah akun tersebut berdiri sendiri, atau bagian dari organisasi:

- Mandiri Akun AWS — Untuk Akun AWS tidak terkait dengan organisasi, Anda dapat memperbarui kontak akun utama Anda sendiri menggunakan Konsol AWS Manajemen, atau melalui AWS CLI & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui kontak Akun AWS utama mandiri.
- Akun AWS dalam organisasi — Untuk akun anggota yang merupakan bagian dari AWS organisasi, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui akun anggota apa pun di organisasi secara terpusat dari AWS Organizations konsol, atau secara terprogram melalui CLI AWS & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui kontak Akun AWS utama di organisasi Anda.

Topik

- Persyaratan nomor telepon dan alamat email
- Perbarui kontak utama untuk mandiri Akun AWS atau akun manajemen
- Perbarui kontak utama untuk apa pun AWS akun anggota di organisasi Anda
- Verifikasi nomor telepon kontak utama

Persyaratan nomor telepon dan alamat email

Sebelum Anda melanjutkan dengan memperbarui informasi kontak utama akun Anda, kami sarankan Anda terlebih dahulu meninjau persyaratan berikut saat memasukkan nomor telepon dan alamat email.

- Nomor telepon seharusnya hanya berisi angka.
- Nomor telepon harus dimulai dengan kode + dan negara dan tidak boleh memiliki nol di depan atau spasi tambahan setelah kode negara. Misalnya, +1 (US/Canada) atau +44 (Inggris).
- Nomor telepon tidak boleh menyertakan spasi antara kode area, kode pertukaran, dan kode lokal. Misalnya, +12025550179.
- Untuk tujuan keamanan, nomor telepon harus mampu menerima SMS dari AWS. Nomor bebas pulsa tidak akan diterima karena sebagian besar tidak mendukung SMS.
- Untuk bisnis Akun AWS, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada satu milik individu. Mengkonfigurasi pengguna root akun dengan alamat email atau nomor telepon individu dapat membuat akun Anda sulit dipulihkan jika individu tersebut meninggalkan perusahaan.

Perbarui kontak utama untuk mandiri Akun AWS atau akun manajemen

Untuk mengedit detail kontak utama Anda untuk akun mandiri Akun AWS atau akun manajemen, lakukan langkah-langkah dalam prosedur berikut. Konsol Manajemen AWS Prosedur berikut selalu berfungsi hanya dalam konteks mandiri. Anda dapat menggunakan Konsol Manajemen AWS untuk mengakses atau mengubah hanya informasi kontak utama dari akun yang Anda gunakan untuk memanggil operasi.

Konsol Manajemen AWS

Untuk mengedit kontak utama Anda untuk standalone Akun AWS atau akun manajemen

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetContactInformation`(untuk melihat detail kontak utama)
> - `account:PutContactInformation`(untuk memperbarui detail kontak utama)

1. Masuk ke Konsol Manajemen AWSsebagai pengguna IAM atau peran yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Gulir ke bawah ke bagian Informasi kontak, dan di sebelahnya pilih Edit.
4. Ubah nilai di salah satu bidang yang tersedia.
5. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak utama dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetContactInformation
- PutContactInformation

Catatan

- Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Akun.

Izin minimum

Untuk setiap operasi, Anda harus memiliki izin yang memetakan operasi itu:

- `account:GetContactInformation`
- `account:PutContactInformation`

Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil informasi kontak utama saat ini untuk akun pemanggil.

```
$ aws account get-contact-information
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

Contoh berikut menetapkan informasi kontak utama baru untuk akun pemanggil.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
 Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Perintah ini tidak menghasilkan output jika berhasil.

Perbarui kontak utama untuk apa pun AWS akun anggota di organisasi Anda

Untuk mengedit detail kontak utama Anda di akun AWS anggota mana pun di organisasi Anda, lakukan langkah-langkah dalam prosedur berikut.

Persyaratan tambahan

Untuk memperbarui kontak utama dengan AWS Organizations konsol, Anda perlu melakukan beberapa pengaturan awal:

- Organisasi Anda harus mengaktifkan semua fitur untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi. Jika organisasi Anda disetel ke penagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat Mengaktifkan semua fitur untuk organisasi.
- Anda perlu mengaktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihatAktifkan akses tepercaya untuk AWS Pengelolaan Akun.

Konsol Manajemen AWS

Untuk mengedit kontak utama Anda untuk setiap Akun AWS di organisasi Anda

1. Masuk ke AWS Organizations konsol dengan kredenal akun manajemen organisasi.
2. Dari Akun AWS, pilih akun yang ingin Anda perbarui.
3. Pilih Info kontak, dan temukan Kontak utama.
4. Pilih Edit.
5. Ubah nilai di salah satu bidang yang tersedia.

6. Setelah Anda membuat semua perubahan, pilih Simpan.

Jika Anda mengubah nomor telepon, kami mengirimkan kode verifikasi ke nomor baru saat Anda memilih Simpan. Anda dapat memverifikasi nomornya segera atau lambat. Untuk informasi selengkapnya, lihat Verifikasi nomor telepon untuk akun anggota di organisasi Anda.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak utama dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetContactInformation
- PutContactInformation

> **Catatan**
>
> - Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Akun.
> - Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan operasi itu:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil informasi kontak utama saat ini untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account get-contact-information --account-id 123456789012
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

Contoh berikut menetapkan informasi kontak utama untuk akun anggota tertentu dalam organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
 "CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
 "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Perintah ini tidak menghasilkan output jika berhasil.

Verifikasi nomor telepon kontak utama

Anda dapat memverifikasi nomor telepon di informasi kontak utama untuk file Akun AWS. Verifikasi mengonfirmasi bahwa nomor telepon pada file dapat menerima pesan teks SMS dari kami.

Saat Anda memulai verifikasi, kami mengirimkan kode verifikasi 6 digit melalui pesan teks SMS ke nomor telepon yang saat ini ada di file untuk akun tersebut. Anda tidak memasukkan nomor telepon untuk memulai verifikasi. Untuk menyelesaikannya, Anda memasukkan kode sebelum kedaluwarsa.

Ingatlah hal berikut saat Anda memverifikasi nomor telepon:

- Kode kedaluwarsa 5 menit setelah kami mengirimkannya.
- Jika Anda meminta kode baru, kode yang kami kirim sebelumnya tidak lagi berfungsi.
- Jika kode salah atau telah kedaluwarsa, minta kode baru dan coba lagi.
- Jika nomor telepon berubah setelah kami mengirim kode, Anda tidak dapat menggunakan kode itu. Minta kode baru untuk nomor saat ini.
- Status verifikasi selalu menggambarkan nomor telepon yang saat ini ada di file. Jika Anda mengubah nomor telepon, status menggambarkan nomor baru.
- Untuk akun anggota di organisasi, kode masuk ke nomor telepon kontak utama akun anggota, bukan ke nomor telepon Anda. Sebelum Anda mulai, pastikan Anda bisa mendapatkan kode dari siapa pun yang memiliki ponsel itu.

Untuk memeriksa status verifikasi, gunakan GetContactInformationoperasi. `VerificationStatus`Bidang dalam respons memiliki salah satu nilai berikut:

- `VERIFIED`— Nomor telepon pada file diverifikasi.
- `UNVERIFIED`— Nomor telepon pada file tidak diverifikasi.
- `NOT_SUPPORTED`— Verifikasi nomor telepon tidak tersedia untuk akun ini.

Verifikasi nomor telepon untuk standalone atau manajemen Akun AWS

Untuk memverifikasi nomor telepon akun yang kredensialnya Anda gunakan, gunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- SendPhoneNumberVerification
- VerifyPhoneNumber

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan operasi itu:

- `account:SendPhoneNumberVerification`
- `account:VerifyPhoneNumber`

Untuk memeriksa status verifikasi, Anda juga perlu`account:GetContactInformation`.

Example

AWS CLI Contoh berikut mengirimkan kode verifikasi ke nomor telepon kontak utama akun pemanggil:

```
$ aws account send-phone-number-verification
{
    "Status": "PENDING"
}
```

Example

AWS CLI Contoh berikut mengirimkan kode untuk menyelesaikan verifikasi:

```
$ aws account verify-phone-number --otp 123456
{
    "Status": "VERIFIED"
}
```

Example

AWS CLI Contoh berikut mengambil status verifikasi nomor telepon kontak utama pemanggil:

```
$ aws account get-contact-information --query VerificationStatus
"VERIFIED"
```

Verifikasi nomor telepon untuk akun anggota di organisasi Anda

Anda dapat memverifikasi nomor telepon akun anggota menggunakan AWS Organizations konsol, SDK AWS CLI, atau AWS SDK. Sebelum Anda mulai, selesaikan langkah-langkahnyaPersyaratan tambahan.

Konsol Manajemen AWS

Untuk memverifikasi nomor telepon kontak utama untuk akun anggota

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetContactInformation`(untuk melihat nomor telepon dan apakah sudah diverifikasi)
> - `account:SendPhoneNumberVerification`(untuk mengirim kode verifikasi)
> - `account:VerifyPhoneNumber`(untuk mengirimkan kode)
>
> Kebijakan `AWSOrganizationsFullAccess` terkelola tidak termasuk `account:SendPhoneNumberVerification` atau`account:VerifyPhoneNumber`. Jika Anda mengandalkan kebijakan tersebut, berikan izin ini secara terpisah.

1. Masuk ke AWS Organizations konsol dengan kredenal akun manajemen organisasi.
2. Dari Akun AWS, pilih akun anggota.
3. Pilih Info kontak, dan temukan Kontak utama.
4. Jika nomor telepon tidak diverifikasi, itu muncul dengan peringatan. Pilih nomor telepon, lalu pilih Verifikasi nomor telepon. Kami mengirim kode 6 digit ke nomor telepon akun anggota.
5. Masukkan kode dalam kode Verifikasi, lalu pilih Verifikasi.

   Jika kode tidak tiba, pilih Kirim ulang kode ketika opsi itu tersedia.

AWS CLI & SDKs

Untuk memverifikasi nomor telepon akun anggota, gunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka, dan tentukan ID akun anggota:

- SendPhoneNumberVerification
- VerifyPhoneNumber

> **Catatan**
>
> - Kredensi yang Anda gunakan harus berasal dari akun manajemen organisasi atau akun admin yang didelegasikan untuk AWS Manajemen Akun.
> - Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan operasi itu:
>
> - `account:SendPhoneNumberVerification`
> - `account:VerifyPhoneNumber`
>
> Untuk memeriksa status verifikasi, Anda juga perlu`account:GetContactInformation`.

Example

AWS CLI Contoh berikut mengirimkan kode verifikasi ke nomor telepon kontak utama dari akun anggota yang ditentukan:

```
$ aws account send-phone-number-verification --account-id 123456789012
{
    "Status": "PENDING"
}
```

Example

AWS CLI Contoh berikut mengirimkan kode yang kami kirim ke nomor telepon akun anggota:

```
$ aws account verify-phone-number --account-id 123456789012 --otp 123456
{
    "Status": "VERIFIED"
}
```

Tampilan Akun AWS pengidentifikasi

Informasi ini adalah tentang melihat Akun AWS pengidentifikasi jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

AWS menetapkan pengidentifikasi unik berikut untuk masing-masing: Akun AWS

Akun AWS ID

Nomor 12 digit, seperti 012345678901, yang secara unik mengidentifikasi sebuah. Akun AWS Banyak AWS sumber daya menyertakan ID akun dalam Nama Sumber Daya Amazon (ARN) mereka. Bagian ID akun membedakan sumber daya dalam satu akun dari sumber daya di akun lain. Jika Anda adalah pengguna AWS Identity and Access Management (IAM), Anda dapat masuk Konsol Manajemen AWS menggunakan ID akun atau alias akun. Meskipun ID akun, seperti informasi pengenal lainnya, harus digunakan dan dibagikan dengan hati-hati, mereka tidak dianggap sebagai informasi rahasia, sensitif, atau rahasia.

ID pengguna kanonik

Pengidentifikasi alfa-numerik, seperti`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`, itu adalah bentuk ID yang dikaburkan. Akun AWS Anda dapat menggunakan ID ini untuk mengidentifikasi Akun AWS saat memberikan akses lintas akun ke bucket dan objek menggunakan Amazon Simple Storage Service (Amazon S3). Anda dapat mengambil ID pengguna kanonik untuk Anda Akun AWS sebagai pengguna root atau pengguna IAM.

Anda harus diautentikasi dengan AWS untuk melihat pengidentifikasi ini.

> **Warning**
>
> Jangan berikan AWS kredensi Anda (termasuk kata sandi dan kunci akses) kepada pihak ketiga yang membutuhkan pengenal Akun AWS Anda untuk berbagi AWS sumber daya dengan Anda. Melakukan hal itu akan memberi mereka akses yang sama ke Akun AWS yang Anda miliki.

Temukan milikmu Akun AWS ID

Anda dapat menemukan Akun AWS ID menggunakan Konsol Manajemen AWS atau AWS Command Line Interface (AWS CLI). Di konsol, lokasi ID akun tergantung pada apakah Anda masuk sebagai pengguna root atau pengguna IAM. ID akun sama apakah Anda masuk sebagai pengguna root atau pengguna IAM.

Menemukan ID akun Anda sebagai pengguna root

Konsol Manajemen AWS

Untuk menemukan milikmu Akun AWS ID saat masuk sebagai pengguna root

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Saat Anda masuk sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.

1. Di bilah navigasi di kanan atas, pilih nama atau nomor akun Anda, lalu pilih Kredensi bilitas keamanan.

   > **Tip**
   >
   > Jika Anda tidak melihat opsi KredenSIAL Keamanan, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

2. Di bawah bagian Detail akun, nomor akun muncul di sebelah Akun AWS ID.

AWS CLI & SDKs

Untuk menemukan Akun AWS ID Anda menggunakan AWS CLI

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- Ketika Anda menjalankan perintah sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.

Gunakan perintah get-caller-identity sebagai berikut.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Menemukan ID akun Anda sebagai pengguna IAM

Konsol Manajemen AWS

Untuk menemukan milikmu Akun AWS ID saat masuk sebagai pengguna IAM

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetAccountInformation`

1. Di bilah navigasi di kanan atas, pilih nama pengguna Anda dan kemudian pilih Kredensi bilitas keamanan.

   > **Tip**
   >
   > Jika Anda tidak melihat opsi KredenSIAL Keamanan, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

2. Di bagian atas halaman, di bawah Detail akun, nomor akun muncul di sebelah Akun AWS ID.

AWS CLI & SDKs

Untuk menemukan Akun AWS ID Anda menggunakan AWS CLI

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Ketika Anda menjalankan perintah sebagai pengguna atau peran IAM, maka Anda harus memiliki:
>   - `sts:GetCallerIdentity`

Gunakan perintah get-caller-identity sebagai berikut.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Temukan ID pengguna kanonik untuk Anda Akun AWS

Anda dapat menemukan ID pengguna kanonik untuk Akun AWS menggunakan Konsol Manajemen AWS atau. AWS CLI ID pengguna kanonik untuk sebuah Akun AWS khusus untuk akun tersebut. Anda dapat mengambil ID pengguna kanonik untuk Anda Akun AWS sebagai pengguna root, pengguna federasi, atau pengguna IAM.

Temukan ID kanonik sebagai pengguna root atau pengguna IAM

Konsol Manajemen AWS

Untuk menemukan ID pengguna kanonik untuk akun Anda saat masuk ke konsol sebagai pengguna root atau pengguna IAM

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- Ketika Anda menjalankan perintah sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.
- Saat Anda masuk sebagai pengguna IAM, maka Anda harus memiliki:
  - `account:GetAccountInformation`

1. Masuk ke Konsol Manajemen AWS sebagai pengguna root atau pengguna IAM.
2. Di bilah navigasi di kanan atas, pilih nama atau nomor akun Anda, lalu pilih Kredensi bilitas keamanan.

> **Tip**
>
> Jika Anda tidak melihat opsi KredenSIAL Keamanan, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

3. Di bawah bagian Detail akun, ID pengguna kanonik muncul di sebelah ID pengguna Canonical. Anda dapat menggunakan ID pengguna kanonik untuk mengonfigurasi daftar kontrol akses (ACL) Amazon S3.

AWS CLI & SDKs

Untuk menemukan ID pengguna kanonik menggunakan AWS CLI

Perintah AWS CLI dan API yang sama berfungsi untuk Pengguna root akun AWS, pengguna IAM, atau peran IAM.

Gunakan perintah list-bucket sebagai berikut.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Menemukan ID kanonik sebagai pengguna federasi dengan peran IAM

Konsol Manajemen AWS

Untuk menemukan ID kanonik untuk akun Anda saat masuk ke konsol sebagai pengguna federasi dengan peran IAM

> **Izin minimum**
>
> - Anda harus memiliki izin untuk membuat daftar dan melihat bucket Amazon S3.

1. Masuk ke Konsol Manajemen AWS sebagai pengguna federasi dengan peran IAM.
2. Di konsol Amazon S3, pilih nama bucket untuk melihat detail tentang bucket.
3. Pilih tab Izin.
4. Di bagian Daftar kontrol akses, di bawah Pemilik Bucket, ID kanonik untuk Anda Akun AWS muncul.

AWS CLI & SDKs

Untuk menemukan ID pengguna kanonik menggunakan AWS CLI

Perintah AWS CLI dan API yang sama berfungsi untuk Pengguna root akun AWS, pengguna IAM, atau peran IAM.

Gunakan perintah list-bucket sebagai berikut.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Memecahkan masalah Anda Akun AWS

Informasi ini adalah tentang memecahkan masalah Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Gunakan informasi dalam topik berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah dengan Anda Akun AWS. Untuk bantuan dengan pengguna root, lihat Mem ecahkan masalah dengan pengguna root di Panduan Pengguna IAM. Untuk bantuan tentang proses masuk, lihat Memec ahkan Akun AWS masalah masuk di Panduan AWS Sign-In Pengguna.

Topik-topik penyelesaian masalah

- Memecahkan masalah dengan Akun AWS pembuatan
- Memecahkan masalah dengan Akun AWS penutupan
- Memecahkan masalah lain dengan Akun AWS

Memecahkan masalah dengan Akun AWS pembuatan

Informasi ini adalah tentang pemecahan masalah dengan Akun AWS pembuatan jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Gunakan tautan referensi dalam tabel berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah dengan membuat yang baru Akun AWS.

Isu	Tautan referensi	Sumber
Saya tidak tahu cara mendaftar atau membuat akun	Daftar untuk AWS (lanjutan)	Panduan ini
Apa yang harus saya lakukan jika saya tidak menerima panggilan AWS untuk memverifikasi akun baru saya atau PIN yang saya masukkan tidak berfungsi?	https://repost.aws/knowledge-center/phone-verify-no-call	AWS re:Post

Isu	Tautan referensi	Sumber
Bagaimana cara mengatasi kesalahan “jumlah maksimum upaya gagal” ketika saya mencoba memverifikasi Akun AWS melalui telepon?	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post
Sudah lebih dari 24 jam dan akun saya tidak diaktifkan	https://repost.aws/knowledge-center/create-and-activate-aws-account	AWS re:Post
Saya tidak dapat masuk ke akun baru saya setelah dibuat	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html	AWS Sign-In Panduan Pengguna

Untuk bantuan tambahan, kami sarankan Anda AWS re:Post mencari konten yang terkait dengan masalah spesifik Anda. Jika Anda masih membutuhkan bantuan, hubungi AWS Dukungan.

Memecahkan masalah dengan Akun AWS penutupan

Informasi ini adalah tentang pemecahan masalah dengan Akun AWS penutupan jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Gunakan informasi di bawah ini untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang ditemukan selama proses penutupan akun. Untuk informasi umum tentang proses penutupan akun, lihatTutup Akun AWS.

Topik

- Saya tidak tahu cara menghapus atau membatalkan akun saya
- Saya tidak melihat tombol Tutup akun di halaman Akun
- Saya menutup akun saya tetapi masih belum menerima konfirmasi email
- Saya menerima kesalahan ConstraintViolationException "" ketika mencoba menutup akun saya
- Saya menerima kesalahan “CLOSE_ACCOUNT_QUOTA_EXCEEDED” saat mencoba menutup akun anggota

- Apakah saya perlu menghapus AWS organisasi sebelum menutup akun manajemen?

Saya tidak tahu cara menghapus atau membatalkan akun saya

Untuk menutup akun Anda, ikuti instruksi diTutup Akun AWS.

Saya tidak melihat tombol Tutup akun di halaman Akun

Jika Anda tidak masuk sebagai pengguna root, Anda tidak akan melihat tombol Tutup akun ditampilkan di halaman Akun. Anda harus Masuk Konsol Manajemen AWS sebagai pengguna root untuk menutup akun Anda. Jika Anda tidak dapat masuk, lihat Mem ecahkan masalah dengan pengguna root.

Saya menutup akun saya tetapi masih belum menerima konfirmasi email

Email konfirmasi ini hanya dikirim ke alamat email pengguna root alamat email untuk Akun AWS. Jika Anda tidak menerima email ini dalam beberapa jam, Anda dapat Masuk ke Konsol Manajemen AWS sebagai pengguna root untuk memeriksa apakah akun Anda ditutup. Jika akun Anda berhasil ditutup, Anda akan melihat pesan ditampilkan yang menunjukkan akun Anda ditutup. Jika akun yang Anda tutup adalah akun anggota, Anda dapat memverifikasi penutupan yang berhasil dengan memeriksa apakah akun yang ditutup diberi label seperti `CLOSED` di AWS Organizations konsol. Untuk informasi selengkapnya, lihat Menutup akun anggota di organisasi Anda di Panduan AWS Organizations Pengguna.

Jika Anda mencoba menutup akun manajemen dan tidak menerima konfirmasi email tentang penutupan akun, organisasi Anda kemungkinan besar memiliki akun anggota aktif. Anda hanya dapat menutup akun manajemen jika organisasi Anda tidak memiliki akun anggota aktif. Untuk memverifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda, buka AWS Organizations konsol, dan pastikan bahwa semua akun anggota ditampilkan di `Closed` samping nama akun mereka. Setelah itu, Anda dapat menutup akun manajemen.

Saya menerima kesalahan ConstraintViolationException "" ketika mencoba menutup akun saya

Anda mencoba menutup akun manajemen menggunakan AWS Organizations konsol, yang tidak mungkin. Untuk menutup akun manajemen, Anda perlu Masuk ke Konsol Manajemen AWS sebagai pengguna root untuk akun manajemen dan menutupnya dari halaman Akun. Untuk informasi selengkapnya, lihat Menutup akun manajemen di organisasi Anda di Panduan AWS Organizations Pengguna.

Saya menerima kesalahan “CLOSE_ACCOUNT_QUOTA_EXCEEDED” saat mencoba menutup akun anggota

Anda hanya dapat menutup 20% akun anggota dalam periode 30 hari bergulir. Kuota ini tidak terikat oleh bulan kalender, tetapi dimulai saat Anda menutup akun. Dalam 30 hari sejak penutupan akun awal tersebut, Anda tidak dapat melebihi batas penutupan akun 20%. Penutupan akun minimum adalah 250 dan penutupan akun maksimum adalah 1000, bahkan jika 20% akun melebihi 1000. Untuk informasi selengkapnya tentang kuota Organisasi, lihat Kuota untuk AWS Organizations di Panduan AWS Organizations Pengguna.

Apakah saya perlu menghapus AWS organisasi sebelum menutup akun manajemen?

Tidak, Anda tidak perlu menghapus AWS organisasi sebelum menutup akun manajemen. Namun, Anda hanya dapat menutup akun manajemen jika organisasi Anda tidak memiliki akun anggota aktif. Untuk memverifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda, buka AWS Organizations konsol, dan pastikan bahwa semua akun anggota ditampilkan di `Closed` samping nama akun mereka. Setelah itu, Anda dapat menutup akun manajemen.

Memecahkan masalah lain dengan Akun AWS

Informasi ini adalah tentang pemecahan masalah lain dengan Anda Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar untuk AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Gunakan informasi di sini untuk membantu Anda memecahkan masalah yang terkait dengan Anda. Akun AWS

Masalah

- Saya perlu mengganti kartu kredit untuk Akun AWS
- Saya perlu melaporkan penipuan Akun AWS aktivitas
- Aku harus menutup Akun AWS
- Saya mendapatkan AccessDeniedExceptionketika saya memperbarui alamat email pengguna root

Saya perlu mengganti kartu kredit untuk Akun AWS

Untuk mengganti kartu kredit Anda Akun AWS, Anda harus dapat masuk. AWS memiliki perlindungan di tempat yang mengharuskan Anda untuk membuktikan bahwa Anda adalah pemilik akun. Untuk petunjuk, lihat Mengelola metode pembayaran kartu kredit Anda di Panduan AWS Billing Pengguna.

Saya perlu melaporkan penipuan Akun AWS aktivitas

Jika Anda mencurigai aktivitas penipuan menggunakan Anda Akun AWS dan ingin membuat laporan, lihat Bagaimana cara melaporkan penyalahgunaan sumber daya. AWS

Jika Anda mengalami masalah dengan pembelian yang dilakukan Amazon.com, lihat Layanan Pelanggan Amazon.

Aku harus menutup Akun AWS

Untuk membantu memecahkan masalah dengan menutup masalah Anda Akun AWS, lihat. Tutup Akun AWS

Saya mendapatkan **`AccessDeniedException`**ketika saya memperbarui alamat email pengguna root

Jika akun anggota adalah akun proyek, Anda tidak dapat memperbarui alamat email pengguna root. ID AWS Builder memiliki setiap akun proyek, bukan alamat email pengguna root. Lihat informasi yang lebih lengkap di Akun proyek setelah Anda mengaktifkan fitur lanjutan.

Kelola akun di India

Informasi ini tentang mengelola akun di India jika Anda mendaftar untuk AWS menggunakan Daftar AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Jika Anda mendaftar untuk yang baru Akun AWS dan memilih India untuk kontak dan alamat penagihan Anda, perjanjian pengguna Anda adalah dengan Amazon Web Services India Private Limited (AWS India), AWS penjual lokal di India. AWS India mengelola tagihan Anda, dan total faktur Anda tercantum dalam rupee India (INR), bukan dolar AS (USD). Untuk informasi tentang mengelola Akun AWS, lihatKonfigurasikan Anda Akun AWS.

Jika akun Anda AWS di India, ikuti prosedur dalam topik ini untuk mengelola akun Anda. Topik ini menjelaskan cara mendaftar untuk akun AWS India, mengedit informasi tentang akun AWS India Anda, mengelola verifikasi pelanggan, dan menambahkan atau mengedit Nomor Akun Permanen (PAN) Anda.

Sebagai bagian dari verifikasi kartu kredit saat mendaftar, AWS India menagih kartu kredit Anda 2 INR. AWS India mengembalikan 2 INR setelah verifikasi selesai. Anda mungkin akan dialihkan ke bank sebagai bagian dari proses verifikasi.

Topik

- Buat sebuah Akun AWS dengan AWS India
- Kelola informasi verifikasi pelanggan Anda

Buat sebuah Akun AWS dengan AWS India

AWS India adalah penjual lokal AWS di India. Jika kontak dan alamat penagihan Anda berada di India dan Anda ingin membuat akun, gunakan prosedur berikut untuk mendaftar akun AWS India.

Untuk mendaftar untuk AWS Akun India

1. Buka halaman beranda Amazon Web Services.
2. Pilih Buat Akun AWS.

   > **Note**
   >
   > Jika Anda masuk AWS baru-baru ini, opsi itu mungkin tidak ada. Sebagai gantinya, pilih Masuk ke Konsol. Jika Buat yang baru Akun AWS masih tidak terlihat, pilih Masuk ke akun lain, lalu pilih Buat yang baru Akun AWS.

3. Masukkan informasi akun Anda, verifikasi alamat email Anda, dan pilih kata sandi yang kuat untuk akun Anda.
4. Pilih Bisnis atau Pribadi. Akun pribadi dan akun bisnis memiliki fitur dan fungsi yang sama.
5. Masukkan informasi kontak perusahaan atau pribadi Anda. Jika kontak atau alamat penagihan Anda berbasis di India, sesuai dengan peraturan Tim Tanggap Darurat Komputer India (CERT-In), AWS diperlukan untuk mengumpulkan dan memvalidasi informasi identitas Anda sebelum memberi Anda akses ke layanan. AWS

   Nama yang Anda pilih antara kontak atau informasi penagihan harus sama persis dengan nama yang muncul pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen. Untuk daftar jenis dokumen yang diterima, lihatthe section called “Dokumen India yang diterima untuk verifikasi pelanggan”.
6. Setelah Anda membaca perjanjian pelanggan, pilih kotak centang syarat dan ketentuan, lalu pilih Lanjutkan.

7. Pada halaman Informasi penagihan, masukkan metode pembayaran yang ingin Anda gunakan. Anda harus memberikan CVV Anda sebagai bagian dari proses verifikasi.
8. Di bawah Apakah Anda memiliki PAN? , pilih Ya jika Anda memiliki Nomor Rekening Permanen (PAN) yang ingin ditampilkan pada faktur pajak Anda, lalu masukkan PAN Anda. Jika Anda tidak memiliki PAN atau ingin menambahkannya setelah mendaftar, pilih No.
9. Pilih Verifikasi dan lanjutkan. AWS India menagih kartu Anda 2 INR sebagai bagian dari proses verifikasi. AWS India mengembalikan 2 INR setelah verifikasi selesai.
10. Pada halaman Konfirmasi identitas Anda, pilih tujuan utama pendaftaran akun Anda.
11. Pilih jenis kepemilikan yang paling mewakili pemilik akun. Jika Anda memilih perusahaan, organisasi, atau kemitraan sebagai jenis kepemilikan, masukkan nama orang manajerial kunci. Orang manajerial utama dapat menjadi direktur, kepala operasi, atau orang yang bertanggung jawab atas operasi dalam bisnis Anda.
12. Bergantung pada jenis kepemilikan yang Anda pilih, pilih jenis dokumen India yang diterima untuk digunakan untuk verifikasi dan ketikkan informasi dokumen Anda.

    > **Note**
    >
    > Jika Anda memiliki akun pribadi dan berencana untuk menggunakan SIM yang tidak dikeluarkan oleh Uni India, sebaiknya gunakan jenis dokumen pribadi yang berbeda untuk verifikasi.

13. Pilih nama yang ingin Anda gunakan untuk verifikasi pelanggan.

    Nama-nama dari informasi penagihan dan kontak Anda akan muncul untuk dipilih jika dikaitkan dengan alamat India. Pastikan nama yang Anda pilih cocok dengan nama pada jenis dokumen yang akan digunakan untuk verifikasi pelanggan. Jika Anda perlu membuat perubahan pada nama yang terkait dengan tagihan atau alamat kontak Anda, Anda dapat melakukannya setelah Anda menyelesaikan pendaftaran akun.
14. Berikan persetujuan Anda untuk mengirimkan informasi untuk verifikasi, lalu pilih Lanjutkan.

    Anda akan diberitahu tentang hasil verifikasi pelanggan melalui email setelah Anda menyelesaikan pendaftaran akun. Anda juga dapat memeriksa status pada halaman verifikasi Pelanggan di pengaturan akun Anda atau di Dasbor AWS Kesehatan nanti. Anda harus lulus verifikasi pelanggan untuk mengakses AWS layanan.
15. Pilih apakah Anda ingin memverifikasi nomor ponsel Anda melalui Pesan teks (SMS) atau Panggilan suara.

16. Pilih kode negara atau wilayah Anda, lalu masukkan nomor ponsel Anda.
17. Lengkapi pemeriksaan keamanan.
18. Pilih Kirim SMS atau Hubungi Saya Sekarang. Setelah beberapa saat, Anda akan menerima pin empat digit dalam SMS atau panggilan otomatis di ponsel Anda.
19. Pada halaman Konfirmasi identitas Anda, masukkan pin yang Anda terima dan pilih Lanjutkan.
20. Pada halaman Pilih paket dukungan, pilih paket dukungan Anda, lalu pilih Daftar lengkap. Setelah metode pembayaran dan verifikasi pelanggan Anda diverifikasi, akun Anda akan diaktifkan dan Anda akan menerima email yang mengonfirmasi aktivasi akun Anda.

> **Note**
>
> Jika Anda telah menyelesaikan verifikasi pelanggan dan mengedit nama, alamat, atau dokumen yang sebelumnya digunakan untuk memverifikasi identitas Anda, Anda mungkin perlu memperbarui dan menyelesaikan verifikasi pelanggan Anda lagi. Untuk informasi selengkapnya, lihat the section called “Mengedit informasi verifikasi pelanggan Anda”.

Kelola informasi verifikasi pelanggan Anda

Sesuai dengan peraturan Tim Tanggap Darurat Komputer India (CERT-In), AWS diperlukan untuk mengumpulkan dan memvalidasi informasi identitas Anda sebelum memberi Anda akses baru atau lanjutan ke AWS layanan. Identitas Anda harus diverifikasi menggunakan nama dari tagihan India atau alamat kontak yang Anda berikan. Selama verifikasi, AWS akan memeriksa apakah nomor dokumen valid dan apakah nama yang Anda berikan cocok dengan nama yang terkait dengan dokumen yang Anda gunakan untuk verifikasi pelanggan. Nama yang Anda pilih antara kontak atau informasi penagihan harus sama persis dengan nama yang muncul pada dokumen.

Untuk memperbarui nama dan alamat penagihan, lihat halaman Preferensi pembayaran. Untuk memperbarui nama dan alamat kontak Anda, lihatthe section called “Perbarui kontak utama untuk Anda Akun AWS”. Jika Anda mengedit informasi apa pun yang sebelumnya Anda gunakan untuk verifikasi pelanggan, seperti nama atau India-based alamat dari informasi penagihan atau kontak Anda, Anda mungkin perlu memperbarui dan mengirimkan kembali informasi verifikasi pelanggan Anda.

Periksa status verifikasi pelanggan Anda

Anda dapat melihat status verifikasi pelanggan Anda kapan saja di halaman verifikasi Pelanggan. Jika status verifikasi Anda diperlukan Verifikasi atau Verifikasi gagal, buat atau perbarui informasi verifikasi pelanggan Anda dan kirimkan untuk verifikasi.

Jika akun manajemen Anda telah mengaktifkan warisan verifikasi pelanggan, status verifikasi akun Anda mencerminkan status akun tersebut. Anda tidak perlu mengambil tindakan apa pun ketika warisan aktif.

Buat informasi verifikasi pelanggan Anda

Untuk menyelesaikan verifikasi pelanggan, Anda harus memberikan informasi dari dokumen India yang diterima. Untuk daftar jenis dokumen yang diterima, lihatthe section called “Dokumen India yang diterima untuk verifikasi pelanggan”.

1. Masuk ke Konsol Manajemen AWS.
2. Pada bilah navigasi, di sudut kanan atas, pilih nama akun Anda (atau alias), lalu pilih Akun.
3. Di bawah Pengaturan lain, pilih Verifikasi pelanggan.

   Jika Anda belum memberikan informasi verifikasi pelanggan Anda sebelumnya, Anda akan melihat halaman Buat verifikasi pelanggan.
4. Pilih nama yang sama persis dengan nama pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen.
5. Berikan informasi yang tersisa yang diminta di halaman. Bergantung pada jenis dokumen yang Anda pilih, Anda mungkin perlu mengunggah salinan bagian depan dan belakang dokumen. Jika Anda mengunggah file gambar, pastikan semua informasi dalam dokumen terlihat dan terbaca.
6. Pilih Kirim.

   Anda akan diberitahu tentang hasil verifikasi pelanggan dan langkah selanjutnya melalui email atau di Dasbor AWS Kesehatan.

Mengedit informasi verifikasi pelanggan Anda

Anda dapat mengedit informasi verifikasi pelanggan Anda, seperti tujuan utama pendaftaran akun, jenis organisasi Anda, dan nama, jenis dokumen, unggahan dokumen, atau informasi dokumen yang ingin Anda gunakan untuk verifikasi.

Jika Anda mengedit nama atau jenis dokumen yang akan digunakan untuk verifikasi pelanggan, atau memperbarui informasi dokumen apa pun, Anda harus memverifikasi kembali identitas Anda saat menyimpan perubahan.

> **Warisan verifikasi aktif**
>
> Jika akun manajemen Anda telah mengaktifkan warisan verifikasi pelanggan, Anda tidak dapat mengedit atau mengirimkan informasi verifikasi pelanggan Anda sendiri. Informasi verifikasi Anda muncul dalam mode hanya-baca.

1. Masuk ke Konsol Manajemen AWS.
2. Pada bilah navigasi, di sudut kanan atas, pilih nama akun Anda (atau alias), lalu pilih Akun.
3. Di bawah Pengaturan lain, pilih Verifikasi pelanggan.
4. Pilih Edit, lalu perbarui informasi yang ingin Anda ubah.

   Saat Anda memperbarui informasi, perhatikan panduan berikut:

   - Jika Anda memilih nama yang berbeda, nama harus sama persis dengan nama pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen.
   - Jika Anda memilih jenis dokumen yang berbeda, Anda perlu mengunggah salinan bagian depan dan belakang (jika ada) dokumen. Semua informasi dalam unggahan dokumen harus terlihat dan terbaca.
   - Jika Anda memiliki akun pribadi dan berencana untuk menggunakan SIM yang tidak dikeluarkan oleh Uni India, sebaiknya gunakan jenis dokumen pribadi yang berbeda untuk verifikasi.

   Untuk daftar jenis dokumen yang diterima, lihatthe section called “Dokumen India yang diterima untuk verifikasi pelanggan”.

5. Pilih Kirim.

   Jika identitas Anda harus diverifikasi lagi karena jenis perubahan yang Anda simpan, Anda akan diberitahu tentang hasil verifikasi pelanggan dan langkah selanjutnya melalui email. Anda juga dapat melihat hasilnya dengan kembali ke halaman verifikasi Pelanggan atau di Dasbor AWS Kesehatan.

Kelola warisan verifikasi pelanggan untuk AWS Organizations

Dengan AWS Organizations, Anda dapat mengaktifkan warisan verifikasi pelanggan untuk organisasi Anda. Saat Anda mengaktifkan pewarisan, akun India-based anggota di organisasi Anda mewarisi status verifikasi akun manajemen Anda. Mereka tidak perlu menyelesaikan verifikasi pelanggan secara mandiri.

Akun manajemen Anda harus menyelesaikan verifikasi pelanggannya sendiri sebelum dapat mengaktifkan warisan. Setelah Anda mengaktifkan warisan, Anda tidak perlu mengirimkan kembali dokumen verifikasi Anda.

Ketika akun manajemen Anda mengaktifkan warisan verifikasi pelanggan, status verifikasi Anda meluas ke akun India-based anggota di organisasi Anda. Untuk akun anggota tersebut, kami dapat menggunakan atau mengungkapkan informasi verifikasi Anda sebagai tanggapan atas permintaan penegakan hukum atau peraturan.

Mengaktifkan atau menonaktifkan warisan verifikasi pelanggan

Gunakan prosedur berikut untuk mengaktifkan atau menonaktifkan warisan verifikasi pelanggan untuk akun India-based anggota organisasi Anda.

1. Buka Konsol Manajemen AWS di Konsol Manajemen AWS.
2. Pada bilah navigasi, pilih nama akun Anda (atau alias), lalu pilih Akun.
3. Di bawah Pengaturan lain, pilih Verifikasi pelanggan.
4. Di bawah Pengaturan verifikasi pelanggan, aktifkan Warisan untuk mengaktifkan pewarisan atau nonaktifkan untuk menonaktifkannya.
5. Tinjau kotak dialog konfirmasi, lalu konfirmasikan pilihan Anda.

Saat Anda mengaktifkan pewarisan, semua akun India-based anggota di organisasi Anda mewarisi status verifikasi Anda. Saat Anda menonaktifkan warisan, kami mengembalikan status verifikasi

sebelumnya untuk akun anggota yang sebelumnya menyelesaikan verifikasi mereka sendiri. Akun anggota tanpa verifikasi sebelumnya harus menyelesaikan verifikasi pelanggan secara independen.

Verifikasi pelanggan untuk AWS Akun anggota Organizations

Jika akun Anda memiliki India-based kontak atau alamat penagihan, Anda mewarisi status verifikasi akun manajemen. Ini berlaku ketika akun manajemen Anda telah mengaktifkan warisan verifikasi pelanggan. Anda dapat melihat pesan di halaman verifikasi Pelanggan yang mengonfirmasi hal ini.

Ketika warisan aktif, Anda tidak dapat mengirimkan atau mengedit informasi verifikasi pelanggan Anda sendiri. Anda tidak perlu mengambil tindakan apa pun.

Jika akun manajemen Anda menonaktifkan warisan, Anda harus memiliki status verifikasi pelanggan Anda sendiri. Hal yang sama berlaku jika akun Anda meninggalkan organisasi, atau akun manajemen menghapus akun Anda dari organisasi. Jika sebelumnya Anda mengirimkan informasi verifikasi Anda sendiri, kami mengembalikan status verifikasi Anda sebelumnya. Anda tidak perlu mengulangi prosesnya. Restorasi ini hanya berlaku jika nama dan alamat Anda tidak berubah sejak verifikasi terakhir Anda.

Dokumen India yang diterima untuk verifikasi pelanggan

Jenis dokumen berikut yang dikeluarkan oleh pemerintah India diterima untuk verifikasi pelanggan.

> **Note**
>
> Tautan berikut dapat berubah oleh pemerintah.

- Kartu PAN - Tersedia dalam format digital dan fisik, kartu Nomor Rekening Permanen (PAN) berisi pengidentifikasi alfanumerik unik yang dikeluarkan oleh Departemen Pajak Penghasilan India untuk individu, perusahaan, dan entitas. PAN terdiri dari sepuluh karakter, termasuk huruf dan angka, dalam format**`AAAAA1111A`**. Untuk menggunakan dokumen ini untuk verifikasi, Anda juga harus memberikan tanggal lahir (individu) atau tanggal pendirian (bisnis) yang muncul pada dokumen PAN dan mengunggah sisi depan kartu. Anda dapat mengunjungi situs web resmi Departemen Pajak Penghasilan untuk memeriksa validitas PAN Anda.
- ID Pemilih Card/EPIC - Kartu ID pemilih, juga dikenal sebagai Kartu Identitas Foto Pemilih (EPIC), berisi nomor identifikasi unik yang dikeluarkan oleh Komisi Pemilihan India untuk pemilih yang memenuhi syarat di India. ID/EPIC Nomor pemilih terdiri dari sepuluh karakter, termasuk huruf

dan angka. Anda dapat mengunjungi situs resmi Komisi Pemilihan India untuk memeriksa validitas ID pemilih Anda. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus mengunggah sisi depan dan belakang kartu.

- Surat Izin Mengemudi - Jika SIM Anda tidak dikeluarkan oleh Uni India, kami sarankan menggunakan jenis dokumen yang berbeda untuk verifikasi. Nomor SIM terdiri dari 12-16 karakter, termasuk huruf, angka, dan spasi atau tanda hubung. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus memberikan tanggal lahir Anda dan mengunggah sisi depan dan belakang kartu. Anda dapat pergi ke situs Sewa Parivahan Kementerian Transportasi Jalan dan Jalan Raya untuk memeriksa validitas SIM Anda.
- Sertifikat Pendirian - Sertifikat pendirian adalah dokumen yang dikeluarkan oleh Kementerian Urusan Korporat (MCA) yang memberi tanggal pendaftaran bisnis sebagai badan hukum. Sertifikat ini digunakan untuk mengidentifikasi dan melacak perusahaan yang terdaftar di India secara unik. Setiap sertifikat berisi Corporate Identification Number (CIN), yang merupakan pengidentifikasi alfanumerik unik yang terdiri dari 21 karakter, termasuk huruf dan angka. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus mengunggah sertifikat dokumen pendirian. Anda dapat pergi ke portal Kementerian Urusan Korporat untuk memeriksa validitas CIN Anda.

Jenis dokumen India yang berbeda diterima untuk akun pribadi dan bisnis:

- Untuk akun pribadi - kartu PAN, ID pemilih card/EPIC, dan SIM.
- Untuk akun bisnis - kartu PAN dan sertifikat pendirian.

Kelola Anda AWS Akun India

Kecuali untuk tugas-tugas berikut, prosedur untuk mengelola akun Anda sama dengan akun yang dibuat di luar India. Untuk informasi umum tentang mengelola akun Anda, lihatthe section called “Konfigurasikan akun Anda”.

Gunakan Konsol Manajemen AWS untuk melakukan tugas-tugas berikut:

- Menambahkan atau mengedit Nomor Rekening Permanen
- Mengedit beberapa Nomor Akun Permanen
- the section called “Kelola informasi verifikasi pelanggan Anda”
- Edit beberapa Nomor Pajak Barang dan Jasa (GST)
- Lihat faktur pajak

Tutup Akun AWS

Petunjuk ini adalah untuk cara menutup Akun AWS jika Anda mendaftar untuk AWS menggunakan Daftar AWS (lanjutan) atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Jika Anda tidak lagi membutuhkannya Akun AWS, Anda dapat menutupnya kapan saja dengan mengikuti instruksi di bagian ini. Setelah Anda menutupnya, Anda dapat membukanya kembali dalam waktu 90 hari sejak Anda menutup akun. Periode antara hari Anda menutup akun dan ketika menutup akun AWS secara permanen disebut sebagai periode pasca-penutupan.

Apa yang perlu Anda ketahui sebelum menutup akun Anda

Sebelum menutup Anda Akun AWS, Anda harus mempertimbangkan hal berikut:

- Menutup akun Anda akan berfungsi sebagai pemberitahuan penghentian Perjanjian AWS Pelanggan untuk akun ini.
- Anda tidak perlu menghapus sumber daya Akun AWS sebelum menutupnya. Namun, kami sarankan Anda mencadangkan sumber daya atau data apa pun yang ingin Anda simpan. Untuk petunjuk tentang cara membuat cadangan sumber daya tertentu, lihat AWS dokumentasi yang sesuai untuk layanan tersebut.
- Anda dapat membuka kembali akun Anda selama periode pasca-penutupan. Biaya untuk layanan yang tersisa di akun Anda akan dimulai ulang jika Anda membukanya kembali. Anda juga tetap bertanggung jawab atas faktur yang belum dibayar dan Instans Cadangan dan Savings Plans yang belum dibayar.
- Anda tetap bertanggung jawab atas semua biaya dan biaya yang belum dibayar untuk layanan yang dikonsumsi sebelum penutupan akun. Anda akan menerima AWS tagihan pada bulan berikutnya setelah menutup akun Anda. Misalnya, jika Anda menutup akun Anda pada 15 Januari, Anda akan menerima tagihan pada awal Februari untuk penggunaan yang terjadi dari 1 Januari hingga 15 Januari. Anda akan terus menerima faktur untuk Instans Cadangan dan Savings Plans setelah menutup akun Anda hingga habis masa berlakunya.
- Anda tidak akan lagi dapat mengakses AWS layanan yang sebelumnya tersedia di akun Anda. Namun, Anda dapat masuk dan mengakses penutupan Akun AWS selama periode pasca-penutupan hanya untuk melihat informasi penagihan sebelumnya, mengakses pengaturan akun, atau kontak. AWS Dukungan
- Anda tidak dapat menggunakan alamat email yang sama yang terdaftar Akun AWS pada Anda pada saat penutupan sebagai email utama orang lain Akun AWS. Jika Anda ingin menggunakan

alamat email yang sama untuk yang berbeda Akun AWS, kami sarankan untuk memperbaruinya sebelum penutupan. Untuk informasi selengkapnya, lihat Perbarui alamat email pengguna root.

- Anda tidak dapat menggunakan alias akun yang sama dengan yang Anda daftarkan Akun AWS pada saat penutupan untuk yang lain Akun AWS. Untuk menggunakan kembali alias untuk yang lain Akun AWS, hapus alias akun sebelum Anda menutup akun. Untuk informasi selengkapnya, lihat Menggunakan alias untuk Akun AWS ID Anda di Panduan Pengguna IAM.
- Jika Anda telah mengaktifkan otentikasi multi-faktor (MFA) pada pengguna Akun AWS root Anda, atau mengonfigurasi perangkat MFA pada pengguna IAM, MFA tidak akan dihapus secara otomatis saat Anda menutup akun. Jika Anda memilih untuk membiarkan MFA dihidupkan selama periode 90 hari pasca-penutupan, jaga agar perangkat MFA tetap aktif hingga periode pasca-penutupan berakhir jika Anda perlu mengakses akun selama waktu itu. Catatan, perangkat token TOTP perangkat keras tidak dapat dikaitkan dengan pengguna lain setelah penutupan permanen akun Anda. Jika Anda ingin menggunakan token TOTP perangkat keras dengan pengguna lain nanti, Anda memiliki opsi untuk menonaktifkan perangkat MFA perangkat keras sebelum menutup akun. Perangkat MFA untuk pengguna IAM harus dihapus oleh administrator akun.

Pertimbangan tambahan untuk akun anggota

- Saat Anda menutup akun anggota, akun tersebut tidak akan dihapus dari organisasi sampai setelah periode pasca-penutupan. Selama periode pasca-penutupan, akun anggota tertutup masih diperhitungkan dalam kuota akun Anda di organisasi. Untuk menghindari jumlah akun terhadap kuota, lihat Menghapus akun anggota dari organisasi Anda sebelum menutupnya.
- Anda hanya dapat menutup 20% atau 250 akun anggota hingga maksimum 1.000 dalam periode 30 hari bergulir, mana yang lebih tinggi. Kuota ini tidak terikat oleh bulan kalender, tetapi dimulai ketika Anda menutup akun. Untuk informasi selengkapnya tentang kuota Organizations, lihat Kuota untuk. AWS Organizations
- Jika Anda menggunakan AWS Control Tower, Anda harus membatalkan kelola akun anggota sebelum mencoba menutup akun. Lihat Membatalkan kelola akun anggota di Panduan Pengguna AWS Control Tower.

Pertimbangan khusus layanan

- AWS Marketplace langganan tidak dibatalkan secara otomatis pada penutupan akun. Jika Anda memiliki langganan, pertama-tama hentikan semua instance perangkat lunak Anda di langganan. Kemudian, buka halaman Kelola langganan AWS Marketplace konsol dan batalkan langganan Anda.

- Setelah akun ditutup, AWS akan mengirim email harian hingga lima hari sebelum kami menangguhkan domain. Setelah domain ditangguhkan, dan tergantung pada registrar domain, kami akan menghapus domain dalam waktu 30 hari atau melepaskan domain ke pendaftarnya. Untuk informasi selengkapnya, lihat Akun AWS Milik saya ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53.

  Jika alamat email untuk pengguna root akun ini menggunakan domain yang terdaftar melalui Route 53 di akun yang sama ini, jangan tutup akun ini sampai Anda menyelesaikan salah satu tindakan berikut: transfer domain ke yang berbeda Akun AWS, atau perbarui alamat email pengguna root untuk menggunakan domain yang tidak terdaftar di akun ini. Jika tidak, menutup akun akan menangguhkan domain, yang merusak pengiriman email ke alamat pengguna root Anda. Tanpa email, Anda tidak dapat memulihkan akun, dan tanpa akun, Anda tidak dapat mengembalikan domain. Setelah 30 hari, Route 53 menghapus domain secara permanen. Ini juga berlaku untuk akun anggota yang alamat email pengguna root menggunakan domain yang terdaftar di akun ini.
- AWS CloudTrail adalah layanan keamanan dasar. Ini berarti bahwa jejak yang dibuat oleh pengguna dapat terus ada dan mengirimkan peristiwa bahkan setelah Akun AWS ditutup, kecuali pengguna secara eksplisit menghapus jejak di dalamnya sebelum menutupnya. Akun AWS Untuk informasi selengkapnya tentang cara meminta penghapusan jejak Akun AWS setelah ditutup, lihat Akun AWS penutupan dan jejak di Panduan Pengguna. CloudTrail

Cara menutup akun Anda

Anda dapat menutup Anda Akun AWS menggunakan prosedur berikut. Perhatikan, bahwa ada panduan berbeda yang disediakan di setiap tab tergantung pada jenis akun [mandiri, anggota, manajemen, dan AWS GovCloud (US)] yang ingin Anda tutup.

Jika Anda mengalami masalah apa pun selama proses penutupan akun, lihatMemecahkan masalah dengan Akun AWS penutupan.

Standalone account

Akun mandiri adalah akun yang dikelola secara individual yang bukan merupakan bagian dari. AWS Organizations

Untuk menutup akun mandiri dari halaman Akun

1. Masuk ke Konsol Manajemen AWS sebagai pengguna root di Akun AWS yang ingin Anda tutup. Anda tidak dapat menutup akun saat masuk sebagai pengguna atau peran IAM.

2. Pada bilah navigasi di sudut kanan atas, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada halaman Akun, pilih tombol Tutup akun.
4. Ketik ID akun Anda (ditampilkan di bagian atas kotak dialog penutupan) untuk mengonfirmasi bahwa Anda telah membaca dan memahami proses penutupan akun.
5. Pilih tombol Tutup akun untuk memulai proses penutupan akun.
6. Dalam beberapa menit, Anda akan menerima konfirmasi email bahwa akun Anda telah ditutup.

> **Note**
>
> Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

Member account

Akun anggota Akun AWS adalah bagian dari AWS Organizations.

Untuk menutup akun anggota dari AWS Organizations konsol

1. Masuk ke konsol AWS Organizations tersebut.
2. Pada Akun AWShalaman, temukan dan pilih nama akun anggota yang ingin Anda tutup. Anda dapat menavigasi hierarki OU, atau melihat daftar datar akun tanpa struktur OU.
3. Pilih Tutup akun di sebelah nama akun di bagian atas halaman. Opsi ini hanya tersedia ketika AWS organisasi berada dalam mode Semua fitur.

   > **Note**
   >
   > Jika organisasi Anda menggunakan mode penagihan Konsolidasi, Anda tidak akan dapat melihat tombol Tutup akun di konsol. Untuk menutup akun dalam mode penagihan gabungan, masuk ke akun yang ingin Anda tutup sebagai pengguna root. Pada halaman Akun, pilih tombol Tutup akun, masukkan ID akun Anda, lalu pilih tombol Tutup akun.

4. Baca dan pastikan Anda memahami panduan penutupan akun.
5. Masukkan ID akun anggota, lalu pilih Tutup akun untuk memulai proses penutupan akun.

> **Note**
>
> Setiap akun anggota yang Anda tutup akan menampilkan `CLOSED` label di sebelah nama akunnya di AWS Organizations konsol hingga 90 hari setelah tanggal penutupan asli. Setelah 90 hari, akun anggota tidak akan lagi ditampilkan di AWS Organizations konsol.

Untuk menutup akun anggota dari halaman Akun

Secara opsional, Anda dapat menutup akun AWS anggota langsung dari halaman Akun di. Konsol Manajemen AWS Untuk panduan langkah demi langkah, ikuti petunjuk di tab Akun mandiri.

Opsi ini tidak tersedia untuk akun proyek, yang tidak memiliki pengguna root. Tutup akun proyek dari AWS Organizations konsol.

Untuk menutup akun anggota menggunakan AWS CLI dan SDK

Untuk petunjuk tentang cara menutup akun anggota menggunakan AWS CLI dan SDK, lihat Menutup akun anggota di organisasi Anda di Panduan AWS Organizations Pengguna.

Management account

Akun manajemen adalah akun Akun AWS yang bertindak sebagai akun induk atau root untuk AWS Organizations.

> **Note**
>
> Anda tidak dapat menutup akun manajemen langsung dari AWS Organizations konsol.

Untuk menutup akun manajemen dari halaman Akun

1. Masuk ke Konsol Manajemen AWS sebagai pengguna root untuk akun manajemen yang ingin Anda tutup. Anda tidak dapat menutup akun saat masuk sebagai pengguna atau peran IAM.
2. Verifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda. Untuk melakukan ini, buka AWS Organizations konsol, dan pastikan semua akun anggota ditampilkan di `Closed` sebelah nama akun mereka. Jika Anda memiliki akun anggota yang masih aktif, Anda harus mengikuti panduan penutupan akun yang disediakan di tab Akun Anggota sebelum Anda dapat melanjutkan ke langkah berikutnya.

3. Pada bilah navigasi di sudut kanan atas, pilih nama atau nomor akun Anda, lalu pilih Akun.
4. Pada halaman Akun, pilih tombol Tutup akun.
5. Ketik ID akun Anda (ditampilkan di bagian atas kotak dialog penutupan) untuk mengonfirmasi bahwa Anda telah membaca dan memahami proses penutupan akun.
6. Pilih tombol Tutup akun untuk memulai proses penutupan akun.
7. Dalam beberapa menit, Anda akan menerima konfirmasi email bahwa akun Anda telah ditutup.

> **Note**
>
> Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

AWS GovCloud (US) account

AWS GovCloud (US) Akun selalu ditautkan ke satu standar Akun AWS untuk tujuan penagihan dan pembayaran.

Untuk menutup AWS GovCloud (US) akun

Jika Anda memiliki akun Akun AWS yang ditautkan ke AWS GovCloud (US) akun, Anda harus menutup akun standar sebelum menutup AWS GovCloud (US) akun. Untuk detail selengkapnya, termasuk cara mencadangkan data dan menghindari AWS GovCloud (US) tagihan yang tidak diinginkan, lihat Menutup AWS GovCloud (US) akun di AWS GovCloud (US) Panduan Pengguna.

Apa yang diharapkan setelah Anda menutup akun

Segera setelah Anda menutup akun Anda, hal berikut akan terjadi:

- Anda akan menerima email yang mengonfirmasi penutupan akun ke alamat email pengguna root. Jika Anda tidak menerima email ini dalam beberapa jam, lihatMemecahkan masalah dengan Akun AWS penutupan.
- Setiap akun anggota yang Anda tutup akan menampilkan `CLOSED` label di sebelah nama akunnya di AWS Organizations konsol hingga 90 hari setelah tanggal penutupan asli. Setelah 90 hari, akun anggota tidak akan lagi ditampilkan di AWS Organizations konsol.

- Jika Anda telah memberikan izin untuk mengakses layanan di akun Anda Akun AWS ke akun lain, permintaan akses apa pun yang dibuat dari akun tersebut akan gagal setelah penutupan akun. Jika Anda membuka kembali Akun AWS, orang lain Akun AWS dapat kembali mengakses AWS layanan dan sumber daya akun Anda jika Anda memberikan izin yang diperlukan kepada mereka.

Penutupan akun mungkin tidak segera terjadi di semua Wilayah dan layanan dan dapat memakan waktu beberapa jam untuk menyelesaikannya.

Post-closure periode

Periode pasca-penutupan mengacu pada lamanya waktu antara hari Anda menutup akun Anda dan ketika menutup akun Anda AWS secara permanen. Akun AWS Periode pasca-penutupan adalah 90 hari. Selama periode pasca-penutupan, Anda dapat mengakses konten dan AWS layanan Anda hanya dengan membuka kembali akun Anda. Setelah periode pasca-penutupan, tutup AWS secara permanen Akun AWS, dan Anda tidak dapat lagi membukanya kembali. AWS juga akan menghapus konten dan sumber daya di akun Anda (kecuali untuk CloudTrail jejak). Setelah akun ditutup secara permanen, Akun AWS ID-nya tidak akan pernah dapat digunakan kembali.

Membuka kembali Akun AWS

Akun Anda akan ditutup secara permanen dalam 90 hari, setelah itu Anda tidak akan dapat membuka kembali akun Anda dan AWS akan menghapus konten yang tersisa di akun Anda. Untuk membuka kembali akun Anda sebelum ditutup secara permanen, lihatBuka kembali Akun AWS.

> **Note**
>
> Biaya untuk layanan yang tersisa di akun Anda akan dimulai ulang jika Anda membukanya kembali.

Buka kembali Akun AWS

Jika Anda menutup Akun AWS dan tidak memiliki saldo terutang, Anda dapat membukanya kembali sendiri selama periode pasca-penutupan.

Anda membuka kembali akun Anda dengan masuk sebagai pengguna root dan mengirimkan permintaan dari halaman Akun.

Apa yang perlu Anda ketahui sebelum membuka kembali akun Anda

Sebelum Anda membuka kembali Akun AWS, perhatikan hal berikut:

- Self-service persyaratan: Anda dapat menggunakan proses swalayan ini hanya jika Anda menutup akun sendiri dan akun Anda tidak memiliki saldo terutang pada saat penutupan akun. Anda harus masuk sebagai pengguna root akun yang ditutup; Anda tidak dapat membuka kembali akun saat masuk sebagai pengguna atau peran IAM. Anda harus mengirimkan permintaan pembukaan kembali Anda dalam waktu 90 hari sejak penutupan akun, selama periode pasca-penutupan.
- Akun ditutup oleh AWS: Jika akun AWS ditutup, Anda tidak dapat membukanya kembali sendiri. Bayar saldo terutang dalam waktu 30 hari sejak tanggal akun Anda ditutup, lalu hubungi AWS Dukunganuntuk membuka kembali akun Anda.
- Pembayaran dan biaya: Akun Anda harus memiliki metode pembayaran yang valid dan belum kedaluwarsa. Karena tagihan bulan sebelumnya diselesaikan pada awal bulan berikutnya, Anda mungkin memiliki saldo terutang untuk penggunaan sebelum penutupan bahkan jika akun Anda tidak memiliki saldo saat penutupan. Untuk meninjau atau membayar saldo, lihat Melakukan pembayaran. Ketika Anda membuka kembali akun Anda, biaya resume untuk layanan apa pun yang masih berjalan di dalamnya. Jika Anda tidak menghentikan layanan ini sebelum menutup akun, Anda mungkin telah dikenakan biaya selama periode pasca-penutupan juga.

Cara membuka kembali akun Anda

Ikuti langkah-langkah ini untuk membuka kembali akun Anda yang sudah ditutup.

> **Note**
>
> Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

Untuk membuka kembali akun Anda dari halaman Akun

1. Masuk ke Konsol Manajemen AWS sebagai pengguna root dari tertutup Akun AWS yang ingin Anda buka kembali. Anda tidak dapat membuka kembali akun saat masuk sebagai pengguna atau peran IAM.
2. Buka halaman Akun untuk akun yang ditutup, sebagai berikut: Di spanduk akun tertutup, pilih Buka kembali akun.

3. Di kotak dialog Buka kembali akun, masukkan ID akun yang ditampilkan di kotak dialog untuk mengonfirmasi bahwa Anda ingin membuka kembali akun.
4. Pilih Buka kembali akun untuk mengirimkan permintaan Anda. Sebuah pesan mengonfirmasi bahwa pembukaan kembali akun telah dimulai.
5. Tunggu hingga pembukaan kembali selesai. Ketika akun Anda aktif kembali, sebuah pesan mengonfirmasi bahwa akun telah berhasil dibuka kembali dan bahwa AWS layanan dan penagihan Anda telah dipulihkan.

Jika tidak AWS dapat membuka kembali akun, Anda akan menerima pemberitahuan konsol yang menjelaskan alasan dan cara mengatasinya.

Apa yang diharapkan setelah Anda membuka kembali akun Anda

Setelah Anda mengirimkan permintaan buka kembali, hal berikut terjadi:

- Untuk memeriksa status, segarkan halaman Akun. Saat pembukaan kembali selesai, akun ditampilkan sebagai aktif dan spanduk akun tertutup tidak lagi muncul.
- Setelah akun aktif, AWS kembalikan akses ke layanan dan sumber dayanya, dan penagihan dilanjutkan.

Siapkan akun Anda untuk digunakan setelah dibuka kembali

Beberapa sumber daya dan langganan tidak dikembalikan ke status berjalan secara otomatis. Setelah akun dibuka kembali, Anda mungkin perlu melakukan hal berikut sebelum dapat melanjutkan operasi normal:

- Mulai instans Amazon EC2 yang dihentikan pada penutupan akun. Untuk informasi selengkapnya, lihat Memulai instans di Panduan Pengguna Amazon EC2.
- Pulihkan database Amazon RDS dari snapshot yang dibuat saat penutupan akun.
- Batalkan dan berlangganan kembali AWS Marketplace langganan apa pun. Langganan tidak dipulihkan secara otomatis saat pembukaan kembali akun.

Ketersediaan wilayah

Self-service pembukaan kembali akun tersedia di semua Wilayah komersial.

Keamanan di AWS Pengelolaan Akun

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama AWS antara Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program Kep AWS atuhan Program Kep . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Manajemen Akun, lihat Layanan AWS dalam cakupan berdasarkan program kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Model tanggung jawab bersama ditegakkan untuk semua Akun AWS. Ini termasuk Akun AWS Anda membuat menggunakan AWS pengalaman baru kami dan akun yang Anda buat menggunakan AWS pengalaman lanjutan kami.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Manajemen AWS Akun. Ini menunjukkan kepada Anda cara mengonfigurasi Manajemen Akun untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Manajemen Akun Anda. Beberapa dokumentasi ini hanya relevan untuk akun yang dibuat dengan AWS pengalaman lanjutan kami. Kami akan mengidentifikasi kapan dokumentasi hanya relevan untuk akun yang dibuat dengan AWS pengalaman lanjutan kami.

Topik

- Perlindungan data di AWS Pengelolaan Akun
- AWS PrivateLink untuk AWS Pengelolaan Akun
- Identity and Access Management untuk AWS Pengelolaan Akun
- AWS kebijakan yang dikelola untuk AWS Pengelolaan Akun

- Validasi kepatuhan untuk AWS Pengelolaan Akun
- Ketahanan di AWS Pengelolaan Akun
- Keamanan infrastruktur di AWS Account Management

Perlindungan data di AWS Pengelolaan Akun

Informasi berikut relevan untuk semua Akun AWS.

Model tanggung jawab AWS https://aws.amazon.com/compliance/shared-responsibility-model/ berlaku untuk perlindungan data dalam Manajemen AWS Akun. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data Ket . Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Umum Perlindungan Data (GDPR).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredenSIAL dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di Panduan AWS CloudTrail Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Manajemen Akun atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

AWS PrivateLink untuk AWS Pengelolaan Akun

Informasi berikut relevan untuk semua Akun AWS.

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host AWS sumber daya Anda, Anda dapat mengakses layanan Manajemen AWS Akun dari dalam VPC tanpa harus melintasi internet publik.

Amazon VPC memungkinkan Anda meluncurkan AWS sumber daya di jaringan virtual khusus. Anda dapat menggunakan VPC untuk mengendalikan pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan gateway jaringan. Untuk informasi lebih lanjut tentang Amazon VPC, lihat Panduan Pengguna Amazon VPC.

Untuk menghubungkan Amazon VPC Anda ke Manajemen Akun, Anda harus terlebih dahulu menentukan titik akhir VPC antarmuka, yang memungkinkan Anda menghubungkan VPC Anda ke layanan lain. AWS Titik akhir memberikan konektivitas yang dapat andal, dapat diskalakan, tanpa memerlukan gateway internet, instans terjemahan alamat jaringan (NAT), atau koneksi VPN. Untuk informasi selengkapnya, lihat VPC Endpoint Antarmuka (AWS PrivateLink) dalam Panduan Pengguna Amazon VPC.

Membuat Titik Akhir

Anda dapat membuat titik akhir Manajemen AWS Akun di VPC menggunakan Konsol Manajemen AWS, AWS Command Line Interface (AWS CLI), AWS SDK, API Manajemen AWS Akun, atau CloudFormation.

Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan konsol Amazon VPC atau AWS CLI, lihat Membuat Titik Akhir Antarmuka di Panduan Pengguna Amazon VPC.

> **Note**
>
> Saat Anda membuat titik akhir, tentukan Manajemen Akun sebagai layanan yang ingin Anda sambungkan ke VPC Anda, menggunakan format berikut:
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> Anda harus menggunakan string persis seperti yang ditunjukkan, menentukan Wil `us-east-1` ayah. Sebagai layanan global, Manajemen Akun dihosting hanya di satu Wil AWS ayah itu.

Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan CloudFormation, lihat sumber daya AWS: :EC2: :VPCendPoint di Panduan Pengguna. CloudFormation

Kebijakan Amazon VPC Endpoint

Anda dapat mengontrol tindakan apa yang dapat dilakukan melalui titik akhir layanan ini dengan melampirkan kebijakan titik akhir saat membuat titik akhir Amazon VPC. Anda dapat membuat aturan IAM kompleks dengan melampirkan beberapa kebijakan titik akhir. Untuk informasi selengkapnya, lihat:

- Kebijakan titik akhir Amazon Virtual Private Cloud untuk Manajemen Akun
- Mengontrol Akses ke Layanan dengan Titik Akhir VPC dalam Panduan. AWS PrivateLink

Kebijakan titik akhir Amazon Virtual Private Cloud untuk Manajemen Akun

Informasi berikut relevan untuk semua Akun AWS.

Anda dapat membuat kebijakan titik akhir Amazon VPC untuk Manajemen Akun di mana Anda menentukan hal berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan oleh kepala sekolah.
- Sumber daya untuk melakukan tindakan.

Contoh berikut menunjukkan kebijakan titik akhir Amazon VPC yang memungkinkan satu pengguna IAM bernama Alice di akun 123456789012 untuk mengambil dan mengubah informasi kontak alternatif untuk semua Akun AWS, tetapi menolak izin semua pengguna IAM untuk menghapus informasi kontak alternatif apa pun di akun mana pun.

Jika Anda ingin memberikan akses ke akun yang merupakan bagian dari AWS Organisasi kepada prinsipal yang ada di salah satu akun anggota organisasi, `Resource` elemen tersebut harus menggunakan format berikut:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Untuk informasi selengkapnya tentang membuat kebijakan titik akhir, lihat Meng ontrol Akses ke Layanan dengan Titik Akhir VPC di AWS PrivateLink Panduan.

Identity and Access Management untuk AWS Pengelolaan Akun

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Manajemen Akun. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Informasi berikut adalah tentang Identity and Access Management for AWS Account Management. Informasi ini paling relevan untuk Akun AWS yang Anda buat saat Anda menggunakan AWS pengalaman lanjutan kami atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk mempelajari cara kerja kontrol akses untuk AWS pengalaman baru kami, lihatBandingkan manajemen akses.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana AWS Manajemen Akun bekerja dengan IAM
- Identity-based contoh kebijakan untuk AWS Pengelolaan Akun
- Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Pengelolaan Akun
- Pemecahan masalah AWS Identitas dan akses Manajemen Akun

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Pemecahan masalah AWS Identitas dan akses Manajemen Akun)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana AWS Manajemen Akun bekerja dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Identity-based contoh kebijakan untuk AWS Pengelolaan Akun)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensional dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensional. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensi dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCP) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS Manajemen Akun bekerja dengan IAM

Informasi ini paling relevan untuk Akun AWS yang Anda buat saat Anda menggunakan AWS pengalaman lanjutan kami. Untuk mempelajari cara kerja kontrol akses untuk AWS pengalaman baru kami, lihatBandingkan manajemen akses.

Sebelum Anda menggunakan IAM untuk mengelola akses ke Manajemen Akun, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Manajemen Akun.

Fitur IAM yang dapat Anda gunakan AWS Pengelolaan Akun

Fitur IAM	Dukungan Manajemen Akun
Identity-based kebijakan	Ya
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya

Fitur IAM	Dukungan Manajemen Akun
Kunci kondisi kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Tidak
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Service-linked peran	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Manajemen Akun dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Identity-based kebijakan untuk Manajemen Akun

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Identity-based contoh kebijakan untuk Manajemen Akun

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. Identity-based contoh kebijakan untuk AWS Pengelolaan Akun

Resource-based kebijakan dalam Manajemen Akun

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Manajemen Akun

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Manajemen Akun, lihat Tindakan yang ditentukan oleh Manajemen AWS Akun di Referensi Otorisasi Layanan.

Tindakan kebijakan dalam Manajemen Akun menggunakan awalan berikut sebelum tindakan.

```
account
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
```

```
      "account:action1",
      "account:action2"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang bekerja dengan kontak alternatif Akun AWS seseorang, sertakan tindakan berikut.

```
"Action": "account:*AlternateContact"
```

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. Identity-based contoh kebijakan untuk AWS Pengelolaan Akun

Sumber daya kebijakan untuk Manajemen Akun

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Layanan Manajemen Akun mendukung jenis sumber daya spesifik berikut dalam `Resource` elemen kebijakan IAM untuk membantu Anda memfilter kebijakan dan membedakan antara jenis Akun AWS berikut:

- akun

  `resource`Jenis ini hanya cocok dengan akun mandiri Akun AWS yang bukan akun anggota dalam organisasi yang dikelola oleh AWS Organizations layanan.
- akun InOrganization

`resource`Jenis ini hanya Akun AWS cocok dengan akun anggota dalam organisasi yang dikelola oleh AWS Organizations layanan.

Untuk melihat daftar jenis sumber daya Manajemen Akun dan ARNnya, lihat Sumber daya yang ditentukan oleh Manajemen AWS Akun di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Manajemen AWS Akun.

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. Identity-based contoh kebijakan untuk AWS Pengelolaan Akun

Kunci kondisi kebijakan untuk Manajemen Akun

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Layanan Manajemen Akun mendukung kunci kondisi berikut yang dapat Anda gunakan untuk memberikan pemfilteran halus untuk kebijakan IAM Anda:

- akun: TargetRegion

  Kunci kondisi ini mengambil argumen yang terdiri dari daftar kode AWS Wilayah. Ini memungkinkan Anda memfilter kebijakan agar hanya memengaruhi tindakan yang berlaku pada Wilayah tertentu.
- akun: AlternateContactTypes

  Kunci kondisi ini mengambil daftar jenis kontak alternatif:
  - PENAGIHAN
  - OPERASI

- SEKURITI

  Menggunakan kunci ini memungkinkan Anda memfilter permintaan hanya untuk tindakan yang menargetkan jenis kontak alternatif yang ditentukan.

- akun: AccountResourceOrgPaths

  Kunci kondisi ini mengambil argumen yang terdiri dari daftar jalur melalui hierarki organisasi Anda ke unit organisasi tertentu (OU). Ini memungkinkan Anda memfilter kebijakan untuk hanya memengaruhi akun target di OU yang cocok.

  ```
  o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- akun: AccountResourceOrgTags

  Kunci kondisi ini mengambil argumen yang terdiri dari daftar kunci tag dan nilai. Ini memungkinkan Anda memfilter kebijakan untuk hanya memengaruhi akun yang merupakan anggota organisasi dan yang ditandai dengan kunci dan nilai tag yang ditentukan.

- akun: EmailTargetDomain

  Kunci kondisi ini mengambil argumen yang terdiri dari daftar domain email. Ini memungkinkan Anda memfilter kebijakan agar hanya memengaruhi tindakan yang cocok dengan domain email yang ditentukan. Kunci kondisi ini peka huruf besar/kecil. Anda harus menggunakan `StringEqualsIgnoreCase` alih-alih `StringEquals` di blok kondisi kebijakan untuk mengontrol tindakan berdasarkan domain alamat email target. Berikut adalah contoh kebijakan yang memungkinkan `account:StartPrimaryEmailUpdate` tindakan untuk diselesaikan ketika domain email berisi`example.com`,`company.org`, atau kombinasi kasus apa pun, seperti`EXAMPLE.COM`.

  ```
  {
      "Version": "2012-10-17",
      "Statement": [
          {
              "Sid": "AllowConditionKey",
              "Effect": "Allow",
              "Action": [
                  "account:StartPrimaryEmailUpdate"
              ],
              "Resource": "*",
              "Condition": {
                  "StringEqualsIgnoreCase": {
  ```

```
                    "account:EmailTargetDomain": [
                        "example.com",
                        "company.org"
                    ]
                }
            }
        }
    ]
}
```

Untuk melihat daftar kunci kondisi Manajemen Akun, lihat Kunci kondisi untuk Manajemen AWS Akun di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Manajemen AWS Akun.

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. Identity-based contoh kebijakan untuk AWS Pengelolaan Akun

Daftar kontrol akses di Manajemen Akun

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Attribute-based kontrol akses dengan Manajemen Akun

Mendukung ABAC (tag dalam kebijakan): Tidak

Attribute-based Access Control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik principal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk Manajemen AWS Akun, kontrol akses berbasis tag hanya didukung melalui kunci `account:AccountResourceOrgTags/key-name` kondisi. Kunci `aws:ResourceTag/key-name` kondisi standar tidak didukung untuk API di namespace akun.

Contoh kebijakan JSON menggunakan kunci kondisi yang didukung

Contoh kebijakan berikut memungkinkan akses untuk melihat informasi kontak untuk akun yang ditandai dengan kunci "" dan nilai “CostCenter12345" atau “67890" di organisasi Anda.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "account:GetContactInformation",
            "account:GetAlternateContact"
         ],
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "account:AccountResourceOrgTags/CostCenter":[
                  "12345",
                  "67890"
               ]
            }
         }
      }
   ]
}
```

Untuk informasi selengkapnya tentang ABAC, lihat Mendefinisikan izin berdasarkan atribut dengan otorisasi ABAC dan tutorial IAM: Menentukan izin untuk mengakses AWS sumber daya berdasarkan tag di Panduan Pengguna IAM.

Menggunakan kredensil sementara dengan Manajemen Akun

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka

panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Cross-service izin utama untuk Manajemen Akun

Mendukung sesi akses terusan (FAS): Ya

Sesi akses teruskan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk Manajemen Akun

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

Service-linked peran untuk Manajemen Akun

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Temukan layanan dalam tabel yang `Yes` menyertakan kolom Service-linked peran. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Identity-based contoh kebijakan untuk AWS Pengelolaan Akun

Informasi ini paling relevan untuk Akun AWS yang Anda buat saat Anda menggunakan AWS pengalaman lanjutan kami. Untuk mempelajari cara kerja kontrol akses untuk AWS pengalaman baru kami, lihatBandingkan manajemen akses.

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya Manajemen Akun. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Manajemen Akun, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk Manajemen AWS Akun dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan halaman Akun di Konsol Manajemen AWS
- Menyediakan akses hanya-baca ke halaman Akun di Konsol Manajemen AWS
- Memberikan akses penuh ke halaman Akun di Konsol Manajemen AWS

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Manajemen Akun di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua

permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan halaman Akun di Konsol Manajemen AWS

Untuk mengakses halaman Akun di Konsol Manajemen AWS, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa pengguna dan peran dapat menggunakan konsol Manajemen Akun, Anda dapat memilih untuk melampirkan kebijakan `AWSAccountManagementReadOnlyAccess` atau `AWSAccountManagementFullAccess` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, dalam banyak kasus, Anda dapat memilih untuk mengizinkan akses hanya ke tindakan yang cocok dengan operasi API yang Anda coba lakukan.

Menyediakan akses hanya-baca ke halaman Akun di Konsol Manajemen AWS

Dalam contoh berikut, Anda ingin memberikan pengguna IAM di akses Akun AWS hanya-baca ke halaman Akun di halaman. Konsol Manajemen AWS Pengguna dengan kebijakan ini terlampir tidak dapat melakukan perubahan apa pun.

`account:GetAccountInformation`Tindakan memberikan akses untuk melihat sebagian besar pengaturan di halaman Akun. Namun, untuk melihat AWS Wilayah yang saat ini diaktifkan, Anda juga harus menyertakan `account:ListRegions` tindakan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "GrantReadOnlyAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Memberikan akses penuh ke halaman Akun di Konsol Manajemen AWS

Dalam contoh berikut, Anda ingin memberikan pengguna IAM dalam akses Akun AWS penuh Anda ke halaman Akun di Konsol Manajemen AWS halaman. Pengguna dengan kebijakan ini terlampir dapat mengubah pengaturan untuk akun.

Kebijakan contoh ini dibuat berdasarkan kebijakan contoh sebelumnya dengan menambahkan setiap izin tulis yang tersedia (kecuali CloseAccount), yang memungkinkan pengguna mengubah sebagian besar pengaturan untuk akun, termasuk izin dan izin. `account:EnableRegion` `account:DisableRegion`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Pengelolaan Akun

Informasi ini paling relevan untuk Akun AWS yang Anda buat saat Anda menggunakan AWS pengalaman lanjutan kami. Untuk mempelajari cara kerja kontrol akses untuk AWS pengalaman baru kami, lihatBandingkan manajemen akses.

Untuk diskusi lengkap tentang Akun AWS dan pengguna IAM, lihat Apa itu IAM? di Panduan Pengguna IAM.

Untuk petunjuk tentang cara memperbarui kebijakan yang dikelola pelanggan, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

AWS Kebijakan tindakan Manajemen Akun

Tabel ini merangkum izin yang memberikan akses ke pengaturan akun Anda. Untuk contoh kebijakan yang menggunakan izin ini, lihat Identity-based contoh kebijakan untuk AWS Pengelolaan Akun.

> **Note**
>
> Untuk memberikan akses tulis kepada pengguna IAM ke pengaturan akun tertentu di halaman Akun Konsol Manajemen AWS, Anda harus mengizinkan `GetAccountInformation` izin, selain izin (atau izin) yang ingin Anda gunakan untuk mengubah setelan itu.

Nama izin	Tingkat akses	Deskripsi
`account:ListRegions`	Daftar	Memberikan izin untuk membuat daftar Wilayah yang tersedia.
`account:GetAccount Information`	Baca	Memberikan izin untuk mengambil informasi akun untuk akun.
`account:GetAlterna teContact`	Baca	Memberikan izin untuk mengambil kontak alternatif untuk akun.
`account:GetContact Information`	Baca	Memberikan izin untuk mengambil informasi kontak utama untuk akun.
`account:GetPrimary Email`	Baca	Memberikan izin untuk mengambil alamat email utama akun.
`account:GetRegionO ptStatus`	Baca	Memberikan izin untuk mendapatkan status keikutser taan suatu Wilayah.
`account:AcceptPrim aryEmailUpdate`	Tulis	Memberikan izin untuk menerima pembaruan alamat email utama dari akun

Nama izin	Tingkat akses	Deskripsi
		anggota dalam suatu AWS organisasi.
`account:CloseAccount`	Tulis	Memberikan izin untuk menutup akun. **Note** Ini adalah izin untuk konsol saja. Tidak ada akses API yang tersedia untuk izin ini.
`account:DeleteAlternateContact`	Tulis	Memberikan izin untuk menghapus kontak alternatif untuk akun.
`account:DisableRegion`	Tulis	Memberikan izin untuk menonaktifkan penggunaan Wilayah.
`account:EnableRegion`	Tulis	Memberikan izin untuk mengaktifkan penggunaan Wilayah.
`account:PutAccountName`	Tulis	Memberikan izin untuk memperbarui nama akun.
`account:PutAlternateContact`	Tulis	Memberikan izin untuk memodifikasi kontak alternatif untuk akun.
`account:PutContactInformation`	Tulis	Memberikan izin untuk memperbarui informasi kontak utama untuk akun.

Nama izin	Tingkat akses	Deskripsi
`account:SendPhoneNumberVerification`	Tulis	Memberikan izin untuk mengirim kode verifikasi ke nomor telepon kontak utama untuk akun.
`account:StartPrimaryEmailUpdate`	Tulis	Memberikan izin untuk memulai pembaruan alamat email utama akun anggota dalam suatu AWS organisasi.
`account:VerifyPhoneNumber`	Tulis	Memberikan izin untuk memverifikasi nomor telepon kontak utama untuk akun dengan mengirimkan kode verifikasi.

Pemecahan masalah AWS Identitas dan akses Manajemen Akun

Informasi ini paling relevan untuk Akun AWS yang Anda buat saat Anda menggunakan AWS pengalaman lanjutan kami. Untuk mempelajari cara kerja kontrol akses untuk AWS pengalaman baru kami, lihatBandingkan manajemen akses.

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Manajemen Akun dan IAM.

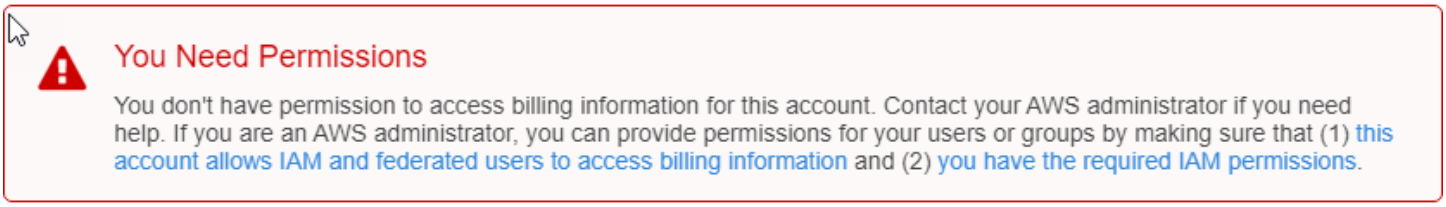
Topik

- Saya tidak berwenang untuk melakukan tindakan di halaman Akun
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses detail akun saya

Saya tidak berwenang untuk melakukan tindakan di halaman Akun

Jika Konsol Manajemen AWS memberi tahu Anda bahwa Anda tidak berwenang untuk melakukan suatu tindakan, maka Anda harus menghubungi administrator Anda untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi Anda.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol untuk melihat detail tentang miliknya Akun AWS di halaman Akun Konsol Manajemen AWS tetapi tidak memiliki `account:GetAccountInformation` izin.



Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *`my-example-widget`* menggunakan tindakan `account:`*`GetWidget`*.

Saya tidak berwenang untuk melakukan **`iam: PassRole`**

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Manajemen Akun.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan dalam Manajemen Akun. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses detail akun saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang

dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Manajemen Akun mendukung fitur ini, lihatBagaimana AWS Manajemen Akun bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

AWS kebijakan yang dikelola untuk AWS Pengelolaan Akun

Informasi ini paling relevan untuk Akun AWS yang Anda buat saat Anda menggunakan AWS pengalaman lanjutan kami atau jika Anda mengaktifkan fitur lanjutan untuk akun Anda. Untuk mempelajari cara kerja kontrol akses untuk AWS pengalaman baru kami, lihatBandingkan manajemen akses.

AWS Manajemen Akun saat ini menyediakan dua AWS kebijakan terkelola yang tersedia untuk Anda gunakan:

- AWS kebijakan yang dikelola: AWSAccountManagementReadOnlyAccess
- AWS kebijakan yang dikelola: AWSAccountManagementFullAccess
- Pembaruan Manajemen Akun ke AWS kebijakan terkelola

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS kebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan ter AWS kelola mungkin tidak memberikan izin hak istimewa terkecil untuk kasus penggunaan spesifik Anda karena kebijakan tersebut tersedia untuk digunakan semua AWS pelanggan. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan ter AWS kelola ketika yang baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan yang dikelola: AWSAccountManagementReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSAccountManagementReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin baca-saja untuk hanya melihat hal-hal berikut:

- Metadata tentang Anda Akun AWS
- Wilayah AWS Yang diaktifkan atau dinonaktifkan untuk Akun AWS (Anda dapat melihat status Wilayah di akun Anda hanya dengan menggunakan AWS konsol)

Ini dilakukan dengan memberikan izin untuk menjalankan salah satu `List*` operasi `Get*` atau. Itu tidak memberikan kemampuan apa pun untuk mengubah metadata akun atau mengaktifkan atau menonaktifkan Wilayah AWS untuk akun.

Detail izin

Kebijakan ini mencakup izin berikut.

- `account`- Memungkinkan kepala sekolah untuk mengambil informasi metadata tentang Akun AWS. Ini juga memungkinkan kepala sekolah untuk membuat daftar Wilayah AWS yang diaktifkan untuk akun di Konsol Manajemen AWS.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan yang dikelola: AWSAccountManagementFullAccess

Anda dapat melampirkan kebijakan `AWSAccountManagementFullAccess` ke identitas IAM Anda.

Kebijakan ini menyediakan akses administratif penuh untuk melihat atau memodifikasi hal-hal berikut:

- Metadata tentang Anda Akun AWS
- Wilayah AWS Yang diaktifkan atau dinonaktifkan untuk Akun AWS (Anda dapat melihat status atau mengaktifkan atau menonaktifkan Wilayah untuk akun Anda hanya dengan menggunakan AWS konsol)

Ini dilakukan dengan memberikan izin untuk menjalankan `account` operasi apa pun.

Detail izin

Kebijakan ini mencakup izin berikut.

- `account`- Memungkinkan kepala sekolah untuk melihat atau memodifikasi informasi metadata tentang Akun AWS. Ini juga memungkinkan kepala sekolah untuk membuat daftar Wilayah AWS yang diaktifkan untuk akun dan mengaktifkan atau menonaktifkannya di Konsol Manajemen AWS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "account:*",
            "Resource": "*"
        }
    ]
}
```

Pembaruan Manajemen Akun ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Manajemen Akun sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Manajemen Akun.

Ubah	Deskripsi	Date
AWS Manajemen Akun diluncurkan dengan kebijakan AWS terkelola baru dan mulai melacak perubahan	Manajemen Akun awalnya diluncurkan dengan kebijakan terkel AWS ola berikut: • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	30 September 2021

Validasi kepatuhan untuk AWS Pengelolaan Akun

Peng AWS alaman baru kami tidak dapat digunakan untuk beban kerja yang diatur. Informasi berikut hanya relevan dengan akun yang dibuat saat Anda menggunakan Daftar untuk AWS (lanjutan).

Third-party auditor menilai keamanan dan kepatuhan AWS layanan yang dapat berjalan di Anda Akun AWS sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat Layanan AWS dalam ruang lingkup berdasarkan program kepatuhan . Untuk informasi umum, lihat Program Kep AWS atuhan Program Jaminan .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Meng AWS Artifact Laporan di Panduan AWS Artifact Pengguna.

Tanggung jawab kepatuhan Anda saat menggunakan layanan Akun AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Merancang untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakannya untuk membuat aplikasi. AWS HIPAA-eligible

  > **Note**
  >
  > Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya Kep — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub CSPM— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.
- AWS Audit Manager— Ini Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Pengelolaan Akun

Informasi berikut relevan untuk semua Akun AWS. Jika Anda menggunakan AWS pengalaman baru kami, pertimbangan Regional tambahan berlaku. Untuk informasi selengkapnya, lihat Wilayah AWS untuk proyek Anda.

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Zona Ketersediaan. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Zona Ketersediaan, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di AWS Account Management

Informasi berikut relevan untuk semua Akun AWS.

Sebagai layanan terkelola, AWS layanan Akun AWS yang berjalan di Anda dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat AWS Keamanan Cloud. Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infra struktur di Security Pillar AWS Well-Architected Framework.

Anda menggunakan panggilan API yang di AWS publikasikan untuk mengakses pengaturan akun melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Suite Cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Pantau Anda Akun AWS

Ini termasuk Akun AWS Anda membuat menggunakan AWS pengalaman baru kami dan akun yang Anda buat menggunakan AWS pengalaman lanjutan kami. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Manajemen AWS Akun dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk memantau Manajemen Akun, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- AWS CloudTrailmenangkap (mencatat) panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS dan menulis file log ke bucket Amazon Simple Storage Service (Amazon S3) yang Anda tentukan. Ini memungkinkan Anda mengidentifikasi pengguna dan akun mana yang AWS dipanggil, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS CloudTrail.
- Amazon EventBridge menambahkan otomatisasi tambahan ke AWS layanan Anda dengan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirim ke EventBridge hampir waktu nyata. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Pencatatan log AWS Panggilan API Manajemen Akun menggunakan AWS CloudTrail

Ini termasuk Akun AWS Anda membuat menggunakan AWS pengalaman baru kami dan akun yang Anda buat menggunakan AWS pengalaman lanjutan kami. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

API Manajemen AWS Akun terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan yang memanggil operasi Manajemen Akun. CloudTrailmenangkap semua panggilan API Manajemen Akun sebagai peristiwa. Panggilan yang ditangkap mencakup semua panggilan ke operasi Manajemen Akun. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk operasi Manajemen Akun. Jika Anda tidak mengonfigurasi

jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol di Ri wayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang disebut operasi Manajemen Akun, alamat IP yang digunakan untuk membuat permintaan, siapa yang membuat permintaan dan kapan, dan detail tambahan.

Untuk mempelajari selengkap CloudTrail nya, lihat Panduan AWS CloudTrail Pengguna.

Informasi Manajemen Akun di CloudTrail

CloudTrail dihidupkan di Anda Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi dengan operasi Manajemen Akun, catat CloudTrail aktivitas tersebut dalam suatu CloudTrail acara bersama dengan peristiwa AWS layanan lainnya di ri wayat acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di Akun AWS. Untuk informasi selengkapnya, lihat Melihat Acara dengan Ri CloudTrail wayat Acara.

Untuk catatan peristiwa yang berkelanjutan di Anda Akun AWS, termasuk acara untuk operasi Manajemen Akun, buat jejak. Jej ak CloudTrail memungkinkan pengiriman file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di Konsol Manajemen AWS, jejak berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengkonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Mener CloudTrail ima file log dari beberapa Wilayah
- M CloudTrail enerima file log dari beberapa akun

AWS CloudTrail mencatat semua operasi API Manajemen Akun yang ditemukan di bagian Referensi API pada panduan ini. Misalnya, panggilan ke`CreateAccount`,`DeleteAlternateContact`, dan `PutAlternateContact` operasi menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan pengguna root atau kredentif pengguna AWS Identity and Access Management (IAM)

- Apakah permintaan dibuat dengan kredentif keamanan sementara untuk peran IAM atau pengguna federasi
- Apakah permintaan dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri log Manajemen Akun

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang operasi yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh 1: Contoh berikut menunjukkan entri CloudTrail log untuk panggilan ke `GetAlternateContact` operasi untuk mengambil kontak `OPERATIONS` alternatif saat ini untuk akun. Nilai yang dikembalikan oleh operasi tidak termasuk dalam informasi yang dicatat.

Example Contoh 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
```

```
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Contoh 2: Contoh berikut menunjukkan entri CloudTrail log untuk panggilan ke `PutAlternateContact` operasi untuk menambahkan kontak `BILLING` alternatif baru ke akun.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
```

```
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Contoh 3: Contoh berikut menunjukkan entri CloudTrail log untuk panggilan ke `DeleteAlternateContact` operasi untuk menghapus kontak `OPERATIONS` alternatif saat ini.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
```

```
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


Memantau acara Manajemen Akun dengan EventBridge

Ini termasuk Akun AWS Anda membuat menggunakan AWS pengalaman baru kami dan akun yang Anda buat menggunakan AWS pengalaman lanjutan kami. Untuk membandingkan opsi pendaftaran, lihatBandingkan opsi pendaftaran.

Amazon EventBridge, sebelumnya disebut CloudWatch Events, membantu Anda memantau peristiwa yang khusus untuk dan memulai tindakan target yang menggunakan yang lain Layanan AWS. Acara dari Layanan AWS dikirim ke EventBridge hampir waktu nyata.

Dengan menggunakan EventBridge, Anda dapat membuat aturan yang cocok dengan peristiwa yang masuk dan merutekan mereka ke target untuk diproses.

Untuk informasi selengkapnya, lihat Mem ulai dengan Amazon EventBridge di Panduan EventBridge Pengguna Amazon.

Acara Manajemen Akun

Contoh berikut menunjukkan peristiwa untuk Manajemen Akun. Acara diproduksi atas dasar upaya terbaik.

Hanya peristiwa yang khusus untuk mengaktifkan dan menonaktifkan Panggilan Wilayah dan API yang saat ini CloudTrail tersedia untuk Manajemen Akun.

Tipe peristiwa

- Acara untuk mengaktifkan dan menonaktifkan Wilayah

Acara untuk mengaktifkan dan menonaktifkan Wilayah

Saat Anda mengaktifkan atau menonaktifkan Wilayah di akun, baik dari Konsol atau dari API, tugas asinkron dimulai. Permintaan awal akan dicatat sebagai CloudTrail peristiwa di akun target. Selain itu, EventBridge acara akan dikirim ke akun panggilan ketika proses aktifkan atau nonaktifkan telah dimulai, dan sekali lagi setelah salah satu proses selesai.

Contoh peristiwa berikut menunjukkan bagaimana permintaan akan dikirim yang menunjukkan bahwa `2020-09-30` di Wil `ap-east-1` ayah adalah `ENABLED` untuk akun`123456789012`.

```
{
   "version":"0",
   "id":"11112222-3333-4444-5555-666677778888",
   "detail-type":"Region Opt-In Status Change",
   "source":"aws.account",
   "account":"123456789012",
   "time":"2020-09-30T06:51:08Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:account::123456789012:account"
   ],
   "detail":{
      "accountId":"123456789012",
      "regionName":"ap-east-1",
      "status":"ENABLED"
   }
```

```
}
```

Ada empat kemungkinan status yang cocok dengan status yang dikembalikan oleh API `GetRegionOptStatus` dan: `ListRegions`

- `ENABLED`— Wilayah telah berhasil diaktifkan untuk yang `accountId` ditunjukkan
- `ENABLING`— Wilayah sedang dalam proses diaktifkan untuk yang `accountId` ditunjukkan
- `DISABLED`— Wilayah telah berhasil dinonaktifkan untuk yang `accountId` ditunjukkan
- `DISABLING`— Wilayah sedang dalam proses dinonaktifkan untuk yang `accountId` ditunjukkan

Contoh pola peristiwa berikut membuat aturan yang menangkap semua peristiwa Wilayah.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ]
}
```

Contoh pola peristiwa berikut membuat aturan yang menangkap hanya `ENABLED` dan peristiwa `DISABLED` Region.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ],
   "detail":{
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

Kuota untuk AWS Account Management

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap AWS layanan.

Informasi kuota berikut adalah untuk proyek yang Anda buat jika Anda menggunakanDaftar untuk AWS (baru). Untuk menyesuaikan kuota, buat tiket dukungan. Untuk informasi selengkapnya, lihat Dukungan proyek.

Sumber daya	Kuota	Dapat Disesuaikan
Jumlah proyek yang Anda miliki di Paket Gratis	29	Tidak
Jumlah proyek yang dapat Anda miliki di Paket Berbayar	299	Tidak
Jumlah orang yang dapat Anda bagikan proyek	500	Tidak
Jumlah undangan proyek yang dapat Anda terima	100	Tidak

Informasi kuota berikut ini untuk Akun AWS Anda buat jika Anda mendaftar menggunakan Daftar (lanjutan). Kecuali dinyatakan lain, setiap kuota adalah Wilayah AWS-spesifik.

Sumber daya	Kuota
Jumlah maksimum `StartPrimaryEmailUpdate` permintaan per akun target	3 per 30 detik
Jumlah kontak alternatif dalam Akun AWS	3 - masing-masing satu untuk`BILLING`,`SECURITY`, dan `OPERATIONS`
Jumlah permintaan region-opt bersamaan per akun	6

Sumber daya	Kuota
Jumlah permintaan region-opt bersamaan per organisasi	50
Tingkat `AcceptPrimaryEmailUpdate` permintaan per akun penelepon	1 per detik, meledak menjadi 1 per detik
Tingkat `DeleteAlternateContact` permintaan per akun	1 per detik, meledak hingga 6 per detik
Tingkat `DisableRegion` permintaan per akun	1 per detik, meledak menjadi 1 per detik
Tingkat `EnableRegion` permintaan per akun	1 per detik, meledak menjadi 1 per detik
Tingkat `GetAccountInformation` permintaan per akun penelepon	3 per detik, meledak hingga 3 per detik
Tingkat `GetAlternateContact` permintaan per akun	10 per detik, meledak hingga 15 per detik
Tingkat `GetContactInformation` permintaan per akun	10 per detik, meledak hingga 15 per detik
Tingkat `GetGovCloudAccountInformation` permintaan per akun	3 per detik, meledak hingga 5 per detik
Tingkat `GetPrimaryEmail` permintaan per akun penelepon	3 per detik, meledak hingga 3 per detik
Tingkat `GetRegionOptStatus` permintaan per akun	5 per detik, meledak hingga 5 per detik
Tingkat `ListRegions` permintaan per akun	5 per detik, meledak hingga 5 per detik
Tingkat `PutAccountName` permintaan per akun penelepon	1 per detik, meledak menjadi 1 per detik

Sumber daya	Kuota
Tingkat `PutAlternateContact` permintaan per akun	5 per detik, meledak hingga 8 per detik
Tingkat `PutContactInformation` permintaan per akun	5 per detik, meledak hingga 8 per detik
Tingkat `StartPrimaryEmailUpdate` permintaan per akun penelepon	1 per detik, meledak menjadi 1 per detik

Riwayat dokumen untuk Panduan Pengguna Manajemen Akun

Tabel berikut menjelaskan rilis dokumentasi untuk Manajemen AWS Akun.

Perubahan	Deskripsi	Tanggal
API verifikasi nomor telepon baru	Anda dapat menggunakan VerifyPhoneNumberAPI baru SendPhoneNumberVerification dan untuk memverifikasi nomor telepon kontak utama. `GetContactInformation` Responsnya juga mencakup `VerificationStatus` bidang baru.	Oktober 1, 2026
Nilai kuota penutupan akun yang diperbarui	Memperbaiki persentase kuota penutupan akun dari 10% menjadi 20% dan minimum dari 10 hingga 250 dalam topik pemecahan masalah.	Juni 23, 2026
API nama akun baru	Support for new`GetAccountInformation`, dan `PutAccountName` API untuk melihat atau memodifikasi nama akun.	April 22, 2025
Akhir dukungan untuk mengedit pertanyaan tantangan keamanan	Menghapus topik Edit pertanyaan tantangan keamanan Anda dari panduan karena dukungan telah berakhir.	Januari 6, 2025
API email utama baru	Support for new`GetPrimaryEmail`,`StartPrim`	Juni 6, 2024

	aryEmailUpdate , dan AcceptPrimaryEmail Update API untuk memperbarui alamat email pengguna root alamat email secara terpusat untuk akun anggota mana pun. AWS Organizations Untuk informasi selengkapnya, lihat Memperbarui alamat email pengguna root untuk akun anggota di Panduan AWS Organizations Pengguna.	
Menulis ulang topik akun tutup	Sepenuhnya merombak seluruh topik akun penutupan termasuk menambahkan langkah-langkah untuk cara menutup akun anggota dan manajemen.	Februari 1, 2024
Akhir dukungan untuk menambahkan pertanyaan tantangan keamanan baru	Menambahkan konten baru yang mencatat bahwa opsi untuk menambahkan pertanyaan tantangan baru telah dihapus dari halaman Akun.	Januari 5, 2024
Akhir dukungan untuk aws-portal namespace	AWS Identity and Access Management (IAM) tindakan yang sebelumnya digunakan untuk mengelola akun Anda (misalnya, aws-portal:ModifyAccount danaws-portal:ViewAccount) telah mencapai akhir dukungan standar.	Januari 1, 2024

Menulis ulang topik Daerah	Merombak seluruh topik Wilayah sepenuhnya termasuk menambahkan kontrol perluas dan ciutkan.	Oktober 8, 2023
Memindahkan topik pengguna root ke Panduan Pengguna IAM	Diskusi konsolidasi tentang pengguna root ke dalam satu topik, menambahkan tautan referensi silang ke topik pengguna root yang dipindahkan ke Panduan Pengguna IAM.	18 September 2023
Bagian baru ditambahkan ke topik kontak akun utama	Menambahkan nomor Telepon baru dan bagian persyaratan alamat email.	12 September 2023
API informasi kontak baru	Support untuk `PutContactInformation` API `GetContactInformation` dan baru.	22 Juli 2022
AWS Manajemen Akun sekarang mendukung pembaruan kontak alternatif melalui AWS Organizations konsol.	Sekarang Anda dapat memperbarui kontak alternatif organisasi Anda melalui AWS Organizations konsol menggunakan izin API Akun yang disediakan oleh kebijakan AWS Organizations terkelola yang diperbarui.	8 Februari 2022
Rilis awal	Rilis awal Panduan Referensi Manajemen AWS Akun	30 September 2021

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