Panduan Pengguna

AWSPenyiapan

AWSPenyiapan: Panduan Pengguna

Table of Contents

Gambaran Umum

Panduan ini memberikan petunjuk untuk membuat yang baruAkun AWSdan mengatur pengguna administratif pertama Anda diAWS IAM Identity Centermengikuti praktik terbaik keamanan terbaru.

SebuahAkun AWSdiperlukan untuk mengaksesLayanan AWSdan berfungsi sebagai dua fungsi dasar:

- Wadah— SebuahAkun AWSadalah wadah untuk semuaAWSsumber daya yang dapat Anda buat sebagaiAWSpelanggan. Saat Anda membuat bucket Amazon Simple Storage Service (Amazon S3) atau database Amazon Relational Database Service (Amazon RDS) untuk menyimpan data Anda, atau instans Amazon Elastic Compute Cloud (Amazon EC2) untuk memproses data Anda, Anda membuatsumber dayadi akun Anda. Setiap sumber daya diidentifikasi secara unik oleh Amazon Resource Name (ARN) yang menyertakan ID akun akun yang berisi atau memiliki sumber daya.
- Batas keamanan— SebuahAkun AWSadalah batas keamanan dasar untuk AndaAWSsumber daya. Sumber daya yang Anda buat di akun Anda hanya tersedia untuk pengguna yang memiliki kredensi untuk akun yang sama.

  Di antara sumber daya utama yang dapat Anda buat di akun Anda adalahidentitas, seperti pengguna dan peran IAM, dan identitas federasi, seperti pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori IAM Identity Center, atau pengguna lain yang mengaksesLayanan AWSdengan menggunakan mandat yang diberikan melalui sumber identitas. Identitas ini memiliki kredensi yang dapat digunakan seseorang untuk masuk, atauautentikasikepadaAWS. Identitas juga memiliki kebijakan izin yang menentukan apa yang orang yang masuk berwenang lakukan dengan sumber daya di akun.

Terminologi

Amazon Web Services (AWS) menggunakan terminologi umum untuk menggambarkan proses masuk. Kami menyarankan Anda membaca dan memahami istilah-istilah ini.

Administrator

Juga disebut sebagai Akun AWS administrator atau administrator IAM. Administrator, biasanya personel Teknologi Informasi (TI), adalah individu yang mengawasiAkun AWS. Administrator memiliki tingkat izin yang lebih tinggi Akun AWS daripada anggota lain dari organisasi mereka. Administrator menetapkan dan mengimplementasikan pengaturan untuk. Akun AWS Mereka juga membuat pengguna IAM atau IAM Identity Center. Administrator memberi pengguna ini kredensi akses mereka dan URL masuk untuk masuk. AWS

Akun

Standar Akun AWS berisi AWS sumber daya Anda dan identitas yang dapat mengakses sumber daya tersebut. Akun dikaitkan dengan alamat email dan kata sandi pemilik akun.

Kredensial

Juga disebut sebagai kredensial akses atau kredensial keamanan. Kredensial adalah informasi yang diberikan pengguna AWS untuk masuk dan mendapatkan akses ke AWS sumber daya. Kredensi dapat mencakup alamat email, nama pengguna, kata sandi yang ditentukan pengguna, ID akun atau alias, kode verifikasi, dan kode otentikasi multi-faktor penggunaan tunggal (MFA). Dalam autentikasi dan otorisasi, sistem menggunakan kredensial untuk mengidentifikasi siapa yang membuat panggilan dan apakah akan mengizinkan akses yang diminta. DalamAWS, kredenal ini biasanya ID kunci akses dan kunci akses rahasia.

Untuk informasi selengkapnya tentang kredensional, lihat Memahami dan mendapatkan kredensional Anda AWS.

> **Note**
>
> Jenis kredensi yang harus dikirimkan pengguna tergantung pada jenis penggunanya.

Kredensi perusahaan

Kredensi yang diberikan pengguna saat mengakses jaringan dan sumber daya perusahaan mereka. Administrator perusahaan Anda dapat mengatur Akun AWS agar dapat diakses dengan kredensi yang sama yang Anda gunakan untuk mengakses jaringan dan sumber daya perusahaan Anda. Kredensi ini diberikan kepada Anda oleh administrator atau karyawan help desk Anda.

Profil

Ketika Anda mendaftar untuk AWS Builder ID, Anda membuat profil. Profil Anda mencakup informasi kontak yang Anda berikan dan kemampuan untuk mengelola perangkat otentikasi multi-faktor (MFA) dan sesi aktif. Anda juga dapat mempelajari lebih lanjut tentang privasi dan cara kami menangani data Anda di profil Anda. Untuk informasi selengkapnya tentang profil Anda dan kaitannya dengan profilAkun AWS, lihat ID AWS Pembuat dan AWS kredenal lainnya.

Pengguna

Pengguna adalah orang atau aplikasi di bawah akun yang melakukan panggilan API ke AWS produk. Setiap pengguna memiliki nama unik di dalam Akun AWS dan satu set kredensi keamanan yang tidak dibagikan dengan orang lain. Kredensial ini terpisah dari kredensial keamanan untuk Akun AWS. Setiap pengguna dikaitkan dengan satu dan hanya satu Akun AWS.

Kredensial pengguna root

Kredensial pengguna root adalah kredenal yang sama yang digunakan untuk masuk ke AWS Management Console sebagai pengguna root. Untuk informasi selengkapnya tentang pengguna root, lihat Pengguna Root.

Kode verifikasi

Kode verifikasi memverifikasi identitas Anda selama proses masuk menggunakan otentikasi multi-faktor (MFA). Metode pengiriman untuk kode verifikasi bervariasi. Mereka dapat dikirim melalui pesan teks atau email. Periksa dengan administrator Anda untuk informasi lebih lanjut.

AWSpengguna dan kredensialnya

Saat berinteraksiAWS, Anda menentukan kredensi AWS keamanan untuk memverifikasi siapa Anda dan apakah Anda memiliki izin untuk mengakses sumber daya yang Anda minta. AWSmenggunakan kredensi keamanan untuk mengautentikasi dan mengotorisasi permintaan.

Misalnya, jika ingin mengunduh file yang dilindungi dari bucket Amazon Simple Storage Service (Amazon S3), kredensial Anda harus mengizinkan akses tersebut. Jika kredensil Anda menunjukkan bahwa Anda tidak berwenang untuk mengunduh file, tolak permintaan AndaAWS. Namun, kredensi keamanan tidak diperlukan untuk mengunduh file di bucket Amazon S3 yang dibagikan secara publik.

Pengguna root

Juga disebut sebagai pemilik akun atau pengguna root akun. Sebagai pengguna root, Anda memiliki akses lengkap ke semua AWS layanan dan sumber daya di AndaAkun AWS. Saat pertama kali membuat akun Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses lengkap ke semua layanan dan sumber daya AWS dalam akun tersebut. Identitas ini adalah pengguna root AWS akun. Anda dapat masuk ke AWS Management Consolesebagai pengguna root menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Untuk petunjuk langkah demi langkah tentang cara masuk, lihat Masuk ke AWS Management Console sebagai pengguna root.

> **Important**
>
> Saat Anda membuatAkun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan saat membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensil pengguna root Anda dan gunakan untuk melakukan tugas-tugas yang hanya dapat dilakukan oleh pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang identitas IAM termasuk pengguna root, lihat Identitas IAM (pengguna, grup pengguna, dan peran).

Pengguna Pusat Identitas IAM

Pengguna IAM Identity Center masuk melalui portal AWS akses. Portal AWS akses atau URL masuk tertentu disediakan oleh administrator atau karyawan help desk Anda. Jika Anda membuat pengguna Pusat Identitas IAM untuk AndaAkun AWS, undangan untuk bergabung dengan pengguna IAM Identity Center dikirim ke alamat email. Akun AWS URL login tertentu disertakan dalam undangan email. Pengguna IAM Identity Center tidak dapat masuk melalui. AWS Management Console Untuk petunjuk langkah demi langkah tentang cara masuk, lihat Masuk ke portal AWS akses.

> **Note**
>
> Kami menyarankan Anda menandai URL masuk khusus untuk portal AWS akses sehingga Anda dapat mengaksesnya dengan cepat nanti.

Untuk informasi selengkapnya tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas IAM?

Identitas federasi

Identitas federasi adalah pengguna yang dapat masuk menggunakan penyedia identitas eksternal (IDP) yang terkenal, seperti Login with Amazon, Facebook, Google, atau iDP lain yang kompatibel dengan OpenID Connect (OIDC). Dengan federasi identitas web, Anda dapat menerima token otentikasi, dan kemudian menukar token itu dengan kredensil keamanan sementara di peta AWS itu ke peran IAM dengan izin untuk menggunakan sumber daya di Anda. Akun AWS Anda tidak masuk dengan AWS Management Console atau AWS mengakses portal. Sebagai gantinya, identitas eksternal yang digunakan menentukan cara Anda masuk.

Untuk informasi selengkapnya, lihat Masuk sebagai identitas federasi.

Pengguna IAM

Pengguna IAM adalah entitas yang Anda buat. AWS Pengguna ini adalah identitas dalam diri Anda Akun AWS yang diberikan izin khusus khusus. Kredensi pengguna IAM Anda terdiri dari nama dan kata sandi yang digunakan untuk masuk ke. AWS Management Console Untuk petunjuk langkah demi langkah tentang cara masuk, lihat Masuk ke pengguna IAM AWS Management Console sebagai.

Untuk informasi selengkapnya tentang identitas IAM termasuk pengguna IAM, lihat Identitas IAM (pengguna, grup pengguna, dan peran).

AWSPengguna ID Builder

Sebagai pengguna AWS Builder ID, Anda secara khusus masuk ke AWS layanan atau alat yang ingin Anda akses. Pengguna AWS Builder ID melengkapi semua yang sudah Akun AWS Anda miliki atau ingin buat. AWSBuilder ID mewakili Anda sebagai pribadi, dan Anda dapat menggunakannya untuk mengakses AWS layanan dan alat tanpaAkun AWS. Anda juga memiliki profil tempat Anda dapat melihat dan memperbarui informasi Anda. Untuk informasi selengkapnya, lihat Untuk masuk dengan AWS Builder ID.

Prasyarat dan pertimbangan

Sebelum memulai proses penyiapan, tinjau persyaratan akun, pertimbangkan apakah Anda memerlukan lebih dari satuAkun AWS, dan pahami persyaratan untuk menyiapkan akun Anda untuk akses administratif di IAM Identity Center.

Akun AWSpersyaratan

Untuk mendaftarAkun AWS, Anda perlu memberikan informasi berikut:

- Nama akun— Nama akun muncul di beberapa tempat, seperti pada faktur Anda, dan di konsol seperti dasbor Penagihan dan Manajemen Biaya danAWS Organizationskonsol.

  Kami menyarankan Anda menggunakan standar penamaan akun sehingga nama akun dapat dengan mudah dikenali dan dibedakan dari akun lain yang mungkin Anda miliki. Jika itu adalah akun perusahaan, pertimbangkan untuk menggunakan standar penamaan sepertiorganisasi-maksud-lingkungan(misalnya,AnyCompany-audit-prod). Jika itu adalah akun pribadi, pertimbangkan untuk menggunakan standar penamaan sepertinama pertama-nama belakang-maksud(misalnya,paulo-santos-testaccount).
- Alamat email— Alamat email ini digunakan sebagai nama login untuk pengguna root akun, dan diperlukan untuk pemulihan akun, seperti lupa kata sandi. Anda harus dapat menerima pesan yang dikirim ke alamat email ini. Sebelum Anda dapat melakukan tugas-tugas tertentu, Anda harus memverifikasi bahwa Anda memiliki akses ke akun email.

  > **Important**
  >
  > Jika akun ini untuk bisnis, kami sarankan Anda menggunakan daftar distribusi perusahaan (misalnya,`it.admins@example.com`). Hindari menggunakan alamat email perusahaan individu (misalnya,`paulo.santos@example.com`). Ini membantu memastikan bahwa perusahaan Anda dapat mengaksesAkun AWSjika seorang karyawan mengubah posisi atau meninggalkan perusahaan. Alamat email dapat digunakan untuk mengatur ulang kredensi pengguna root akun. Pastikan Anda melindungi akses ke daftar atau alamat distribusi ini.
- Nomor telepon— Nomor ini dapat digunakan saat konfirmasi kepemilikan akun diperlukan. Anda harus dapat menerima panggilan di nomor telepon ini.

> **Important**
>
> Jika akun ini untuk bisnis, kami sarankan menggunakan nomor telepon perusahaan alih-alih nomor telepon pribadi. Ini membantu memastikan bahwa perusahaan Anda dapat mengaksesAkun AWSjika seorang karyawan mengubah posisi atau meninggalkan perusahaan.

- Perangkat autentikasi multi-faktor— Untuk mengamankanAWSsumber daya, aktifkan otentikasi multi-faktor (MFA) pada akun pengguna root. Selain kredensi masuk reguler, otentikasi sekunder diperlukan saat MFA diaktifkan, memberikan lapisan keamanan tambahan. Untuk informasi selengkapnya tentang MFA, lihatApa itu MFA?di dalamPanduan Pengguna IAM.
- AWS Supportrencana- Anda akan diminta untuk memilih salah satu paket yang tersedia selama proses pembuatan akun. Untuk deskripsi paket yang tersedia, lihatBandingkanAWS Supportrencana.

Pertimbangan IAM Identity Center

Topik berikut memberikan panduan untuk menyiapkan IAM Identity Center untuk lingkungan tertentu. Pahami panduan yang berlaku untuk lingkungan Anda sebelum Anda melanjutkanBagian 2: Membuat pengguna administratif di IAM Identity Center.

Topik

- Active Directory atau iDP eksternal
- AWS Organizations
- IAM role
- Firewall generasi berikutnya dan gateway web yang aman

Active Directory atau iDP eksternal

Jika Anda sudah mengelola pengguna dan grup di Active Directory atau IdP eksternal, sebaiknya Anda mempertimbangkan untuk menghubungkan sumber identitas ini saat Anda mengaktifkan IAM Identity Center dan memilih sumber identitas Anda. Melakukan hal ini sebelum Anda membuat pengguna dan grup apa pun di direktori Pusat Identitas default akan membantu Anda menghindari konfigurasi tambahan yang diperlukan jika Anda mengubah sumber identitas Anda nanti.

Jika Anda ingin menggunakan Active Directory sebagai sumber identitas Anda, konfigurasi Anda harus memenuhi prasyarat berikut:

- Jika Anda menggunakanAWS Managed Microsoft AD, Anda harus mengaktifkan IAM Identity Center dalam hal yang samaWilayah AWSdi mana AndaAWS Managed Microsoft ADdirektori diatur. IAM Identity Center menyimpan data penugasan di Wilayah yang sama dengan direktori. Untuk mengelola IAM Identity Center, Anda mungkin perlu beralih ke Wilayah tempat IAM Identity Center dikonfigurasi. Juga, perhatikan bahwaAWSportal akses menggunakan URL akses yang sama dengan direktori Anda.
- Gunakan Active Directory yang berada di akun manajemen Anda:

  Anda harus memiliki Konektor AD yang sudah ada atauAWS Managed Microsoft ADdirektori diatur dalamAWS Directory Service, dan itu harus berada dalamAWS Organizationsakun manajemen. Anda hanya dapat menghubungkan satu Konektor AD atau satuAWS Managed Microsoft ADpada suatu waktu. Jika Anda perlu mendukung beberapa domain atau hutan, gunakanAWS Managed Microsoft AD. Untuk informasi selengkapnya, lihat:

  - Hubungkan direktori diAWS Managed Microsoft ADke IAM Identity Centerdi dalamAWS IAM Identity CenterPanduan Pengguna.
  - Menghubungkan direktori yang dikelola sendiri di Active Directory ke IAM Identity Centerdi dalamAWS IAM Identity CenterPanduan Pengguna.
- Gunakan Active Directory yang berada di akun admin yang didelegasikan:

  Jika Anda berencana untuk mengaktifkan admin yang didelegasikan IAM Identity Center dan menggunakan Active Directory sebagai sumber identitas IAM Anda, Anda dapat menggunakan Konektor AD yang ada atauAWS Managed Microsoft ADdirektori diatur dalamAWSdirektori yang berada di akun admin yang didelegasikan.

  Jika Anda memutuskan untuk mengubah sumber IAM Identity Center dari sumber lain ke Active Directory, atau mengubahnya dari Active Directory ke sumber lain, direktori harus berada di (dimiliki oleh) akun anggota administrator yang didelegasikan IAM Identity Center jika ada; jika tidak, itu harus ada di akun manajemen.

AWS Organizations

AndaAkun AWSharus dikelola olehAWS Organizations. Jika Anda belum menyiapkan organisasi, Anda tidak perlu melakukannya. Saat Anda mengaktifkan IAM Identity Center, Anda akan memilih apakah akan memilikinyaAWSbuat organisasi untuk Anda.

Jika Anda sudah menyiapkanAWS Organizations, pastikan semua fitur diaktifkan. Untuk informasi selengkapnya, lihat Mengaktifkan semua fitur di organisasi Anda dalam Panduan Pengguna AWS Organizations.

Untuk mengaktifkan IAM Identity Center, Anda harus masuk keAWS Management Consoledengan menggunakan kredensyal AndaAWS Organizationsakun manajemen. Anda tidak dapat mengaktifkan IAM Identity Center saat masuk dengan kredensi dariAWS Organizationsakun anggota. Untuk informasi lebih lanjut, lihatMembuat dan mengelolaAWSOrganisasidi dalamAWS OrganizationsPanduan Pengguna.

IAM role

Jika Anda telah mengonfigurasi peran IAM diAkun AWS, kami sarankan Anda memeriksa apakah akun Anda mendekati kuota untuk peran IAM. Untuk informasi lebih lanjut, lihatKuota objek IAM.

Jika Anda mendekati kuota, pertimbangkan untuk meminta kenaikan kuota. Jika tidak, Anda mungkin mengalami masalah dengan IAM Identity Center saat Anda menyediakan set izin ke akun yang telah melebihi kuota peran IAM. Untuk informasi tentang cara meminta kenaikan kuota, lihatMeminta kenaikan kuotadi dalamPanduan Pengguna Kuota Layanan.

Firewall generasi berikutnya dan gateway web yang aman

Jika Anda memfilter akses ke spesifikAWSdomain atau endpoint URL dengan menggunakan solusi penyaringan konten web seperti NGFWs atau SWG, Anda harus menambahkan domain atau endpoint URL berikut ke solusi penyaringan konten web Anda allow-list.

Domain DNS spesifik

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

Endpoint URL tertentu

- https://*[direktori Anda]*.awsapps.com/mulai
- https://*[direktori Anda]*.awsapps.com/masuk
- https://*[wilayahmu]*.signin.aws/platform/masuk

Menggunakan beberapaAkun AWS

Akun AWSberfungsi sebagai batas keamanan mendasar diAWS. Mereka berfungsi sebagai wadah sumber daya yang menyediakan tingkat isolasi yang berguna. Kemampuan untuk mengisolasi sumber daya dan pengguna adalah persyaratan utama untuk membangun lingkungan yang aman dan tertata dengan baik.

Memisahkan sumber daya Anda menjadi terpisahAkun AWSmembantu Anda mendukung prinsip-prinsip berikut di lingkungan cloud Anda:

- Kontrol keamanan- Aplikasi yang berbeda dapat memiliki profil keamanan yang berbeda yang memerlukan kebijakan dan mekanisme kontrol yang berbeda. Misalnya, lebih mudah untuk berbicara dengan auditor dan dapat menunjuk ke satuAkun AWSyang menampung semua elemen beban kerja Anda yang tundukStandar Keamanan Industri Kartu Pembayaran (PCI).
- Isolasi— SebuahAkun AWSadalah unit perlindungan keamanan. Potensi risiko dan ancaman keamanan harus terkandung dalamAkun AWStanpa 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 memindahkan mereka untuk berpisahAkun 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 mengandung paparan data yang sangat pribadi dan oleh karena itu dapat membantu dalam kepatuhan denganPeraturan Perlindungan Data Umum (GDPR) Uni Eropa.
- Proses bisnis- Unit bisnis atau produk yang berbeda mungkin memiliki tujuan dan proses yang sama sekali berbeda. Dengan beberapaAkun 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 (menggunakanAWS Organizationsdan penagihan konsolidasi) sementara memiliki item baris dipisahkan olehAkun AWS.
- Alokasi kuota—AWSkuota layanan diberlakukan secara terpisah untuk masing-masingAkun AWS. Memisahkan beban kerja menjadi berbedaAkun AWSmencegah mereka mengkonsumsi kuota satu sama lain.

Semua rekomendasi dan prosedur yang dijelaskan dalam panduan ini sesuai denganAWSKerangka yang Diarsiteksikan dengan Baik. 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 dalam kerangka kerja. Melakukan hal tersebut dapat membantu Anda menskalakan lingkungan dengan aman dan tanpa memengaruhi operasi Anda yang sedang berlangsung seiring pertumbuhan Anda.

Sebelum Anda mulai menambahkan beberapa akun, Anda akan ingin mengembangkan rencana untuk mengelolanya. Untuk itu, kami sarankan Anda menggunakanAWS Organizations, yang merupakan gratisAWSlayanan, untuk mengelola semuaAkun AWSdi organisasi Anda.

AWSjuga menawarkanAWS Control Tower, yang menambahkan lapisanAWSotomatisasi terkelola ke Organisasi dan secara otomatis mengintegrasikannya dengan yang lainAWSlayanan sepertiAWS CloudTrail,AWS Config, AmazonCloudWatch,AWS Service Catalog, dan lainnya. Layanan ini dapat dikenakan biaya tambahan. Untuk informasi lebih lanjut, lihat Harga AWS Control Tower.

Bagian 1: Mengatur yang baruAkun AWS

Instruksi ini akan membantu Anda membuatAkun AWSdan mengamankan kredensi pengguna root. Selesaikan semua langkah sebelum melanjutkan keBagian 2: Membuat pengguna administratif di IAM Identity Center.

Topik

Langkah 1: Mendaftar untukAWSakun

1. Buka https://portal.aws.amazon.com/billing/signup.
2. PilihBuat sebuahAkun AWS.

   > **Note**
   >
   > Jika Anda masukAWSbaru-baru ini, pilihMasuk ke Konsol. Jika opsiBuat yang baruAkun AWStidak terlihat, pilih duluMasuk ke akun lain, dan kemudian pilihBuat yang baruAkun AWS.

3. Masukkan informasi akun Anda, lalu pilihLanjutkan.

   Pastikan Anda memasukkan informasi akun dengan benar, terutama alamat email Anda. Jika salah memasukkan alamat email, Anda tidak dapat mengakses akun.

4. PilihPribadiatauProfesional.

   Perbedaan antara opsi ini hanya pada informasi yang kami minta kepada Anda. Kedua jenis akun memiliki fitur dan fungsi yang sama.

5. Masukkan informasi perusahaan atau pribadi Anda berdasarkan panduan yang diberikan diAkun AWSpersyaratan.
6. Baca dan terimaAWSPerjanjian Pelanggan.
7. PilihBuat Akun dan Lanjutkan.

Pada titik ini, Anda akan menerima pesan email untuk mengonfirmasi bahwaAkun AWSsiap digunakan. Anda dapat masuk ke akun baru Anda dengan menggunakan alamat email dan kata sandi yang Anda berikan saat mendaftar. Namun, Anda tidak dapat menggunakanAWSlayanan sampai Anda selesai mengaktifkan akun Anda.

8. PadaInformasi Pembayaranhalaman, masukkan informasi tentang metode pembayaran Anda. Jika Anda ingin menggunakan alamat yang berbeda dari yang Anda gunakan untuk membuat akun, pilihGunakan alamat barudan masukkan alamat yang ingin Anda gunakan untuk keperluan penagihan.
9. PilihVerifikasi dan Tambah.

> **Note**
>
> Jika alamat kontak Anda ada di India, perjanjian pengguna untuk akun Anda adalah dengan AISPL, lokalAWSpenjual 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. AISPL membebankan biaya metode pembayaran Anda 2 INR sebagai bagian dari proses verifikasi. AISPL mengembalikan 2 INR setelah menyelesaikan verifikasi.

10. Untuk memverifikasi nomor telepon Anda, pilih kode negara atau wilayah Anda dari daftar, dan masukkan nomor telepon tempat Anda dapat dipanggil dalam beberapa menit berikutnya. Masukkan kode CAPTCHA, dan kirimkan.
11. YangAWSsistem verifikasi otomatis memanggil Anda dan memberikan PIN. Masukkan PIN menggunakan ponsel Anda dan kemudian pilihLanjutkan.
12. PilihAWS Supportrencana.

    Untuk deskripsi paket yang tersedia, lihatBandingkanAWS Supportrencana.

    Halaman konfirmasi muncul yang menunjukkan bahwa akun Anda sedang diaktifkan. Ini biasanya hanya membutuhkan waktu beberapa menit tetapi kadang-kadang dapat memakan waktu hingga 24 jam. Selama aktivasi, Anda dapat masuk ke yang baruAkun AWS. Sampai aktivasi selesai, Anda mungkin melihatLengkapi Mendaftartombol. Anda dapat mengabaikannya.

    AWSmengirimkan pesan email konfirmasi saat aktivasi akun selesai. Periksa email dan folder spam Anda untuk pesan email konfirmasi. Setelah Anda menerima pesan ini, Anda memiliki akses penuh ke semuaAWSlayanan.

Langkah 2: Masuk sebagai pengguna root

Saat pertama kali membuatAkun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan saat membuat akun.

> **Important**
>
> Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensil pengguna root Anda dan gunakan untuk melakukan tugas-tugas yang hanya dapat dilakukan oleh pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di Panduan Pengguna IAM.

Untuk masuk sebagai pengguna root

1. Buka konsol AWS Management Console di https://console.aws.amazon.com/.

   > **Note**
   >
   > Jika sebelumnya Anda telah masuk sebagai pengguna root di browser ini, browser Anda mungkin mengingat alamat email untuk fileAkun AWS.
   > Jika Anda telah masuk sebelumnya sebagai pengguna IAM menggunakan browser ini, browser Anda mungkin menampilkan halaman masuk pengguna IAM sebagai gantinya. Untuk kembali ke halaman masuk utama, pilih Masuk menggunakan email pengguna akar.

2. Jika Anda belum masuk sebelumnya menggunakan browser ini, halaman masuk utama muncul. Jika Anda adalah pemilik akun, pilih pengguna Root. Masukkan alamat Akun AWS email Anda yang terkait dengan akun Anda dan pilih Berikutnya.
3. Anda mungkin diminta untuk menyelesaikan pemeriksaan keamanan. Selesaikan ini untuk pindah ke langkah berikutnya. Jika Anda tidak dapat menyelesaikan pemeriksaan keamanan, coba dengarkan audio atau segarkan pemeriksaan keamanan untuk set karakter baru.
4. Masukkan kata sandi Anda dan pilih Masuk.

Langkah 3: Aktifkan MFA untukAkun AWSpengguna root

Untuk meningkatkan keamanan kredensi pengguna root Anda, kami sarankan Anda mengikuti praktik terbaik keamanan untuk mengaktifkan otentikasi multi-faktor (MFA) untuk AndaAkun AWS. Karena pengguna root dapat melakukan operasi sensitif di akun Anda, menambahkan lapisan otentikasi tambahan ini membantu Anda mengamankan akun dengan lebih baik. Beberapa jenis MFA tersedia.

Untuk petunjuk tentang mengaktifkan MFA untuk pengguna root, lihatMengaktifkan perangkat MFA untuk pengguna diAWSdi dalamPanduan Pengguna IAM.

Bagian 2: Membuat pengguna administratif di IAM Identity Center

Setelah Anda selesaiBagian 1: Mengatur yang baruAkun AWS, langkah-langkah berikut akan membantu Anda mengaturAkun AWSakses untuk pengguna administratif, yang akan digunakan untuk melakukan tugas sehari-hari.

> **Note**
>
> Topik ini menyediakan langkah-langkah minimum yang diperlukan untuk berhasil mengatur akses administrator untukAkun AWSdan membuat pengguna administratif di IAM Identity Center. Untuk informasi tambahan, lihatMemulaidi dalamAWS IAM Identity CenterPanduan Pengguna.

Topik

Langkah 1: Aktifkan IAM Identity Center

> **Note**
>
> Jika Anda tidak mengaktifkan otentikasi multi-faktor (MFA) untuk pengguna root Anda, lengkapiLangkah 3: Aktifkan MFA untukAkun AWSpengguna rootsebelum Anda melanjutkan.

Untuk mengaktifkan IAM Identity Center

1. Masuk keAWS Management Consolesebagai pemilik akun dengan memilihPengguna rootdan memasukiAkun AWSalamat email. Di laman berikutnya, masukkan kata sandi Anda.
2. BukaKonsol IAM Identity Center.

3. Di bawahAktifkan IAM Identity Center, pilihAktifkan.
4. IAM Identity Center membutuhkanAWS Organizations. Jika Anda belum menyiapkan organisasi, Anda harus memilih apakah akan memilikinyaAWSmembuat satu untuk Anda. PilihBuatAWSorganisasiuntuk menyelesaikan proses ini.

   AWS Organizationssecara otomatis mengirimkan email verifikasi ke alamat yang terkait dengan akun manajemen Anda. Mungkin ada waktu tunda sebelum Anda menerima email verifikasi. Verifikasi alamat email Anda dalam waktu 24 jam.

> **Note**
>
> Jika Anda menggunakan lingkungan multi-akun, sebaiknya konfigurasikan administrasi yang didelegasikan. Dengan administrasi yang didelegasikan, Anda dapat membatasi jumlah orang yang memerlukan akses ke akun manajemenAWS Organizations. Untuk informasi lebih lanjut, lihatAdministrasi Delegasidi dalamAWS IAM Identity CenterPanduan Pengguna.

Langkah 2: Pilih sumber identitas Anda

Sumber identitas Anda di IAM Identity Center menentukan lokasi pengguna dan grup Anda dikelola. Anda dapat memilih salah satu dari yang berikut sebagai sumber identitas Anda:

- Direktori IAM Identity Center- Ketika Anda mengaktifkan IAM Identity Center untuk pertama kalinya, secara otomatis dikonfigurasi dengan direktori IAM Identity Center sebagai sumber identitas default Anda. Di sinilah Anda membuat pengguna dan grup dan menetapkan tingkat akses mereka ke akun dan aplikasi AWS Anda.
- Direktori Aktif— Pilih opsi ini jika Anda ingin terus mengelola pengguna di direktori AWS Managed Microsoft AD menggunakan AWS Directory Service atau direktori yang dikelola sendiri di Active Directory (AD).
- Penyedia identitas eksternal- Pilih opsi ini jika Anda ingin mengelola pengguna di penyedia identitas eksternal (IdP) seperti Okta atau Azure Active Directory.

Setelah Anda mengaktifkan IAM Identity Center, Anda harus memilih sumber identitas Anda. Sumber identitas yang Anda pilih menentukan di mana IAM Identity Center mencari pengguna dan grup yang memerlukan akses masuk tunggal. Setelah Anda memilih sumber identitas Anda, Anda akan membuat atau menentukan pengguna dan menetapkan mereka izin administratif untukAkun AWS.

> **Important**
>
> Jika Anda sudah mengelola pengguna dan grup di Active Directory atau penyedia identitas eksternal (IdP), sebaiknya pertimbangkan untuk menghubungkan sumber identitas ini saat Anda mengaktifkan IAM Identity Center dan memilih sumber identitas Anda. Ini harus dilakukan sebelum Anda membuat pengguna dan grup apa pun di direktori Pusat Identitas default dan membuat tugas apa pun. Jika Anda sudah mengelola pengguna dan grup dalam satu sumber identitas, mengubah ke sumber identitas yang berbeda dapat menghapus semua tugas pengguna dan grup yang Anda konfigurasikan di IAM Identity Center. Jika ini terjadi, semua pengguna, termasuk pengguna administratif di IAM Identity Center, akan kehilangan akses masuk tunggal ke akses akses merekaAkun AWSdan aplikasi.

Topik

Hubungkan Active Directory atau IdP lain dan tentukan pengguna

Jika Anda sudah menggunakan Active Directory atau penyedia identitas eksternal (IdP), topik berikut akan membantu Anda menghubungkan direktori Anda ke IAM Identity Center.

Anda dapat menghubungkanAWS Managed Microsoft ADdirektori, direktori yang dikelola sendiri di Active Directory, atau iDP eksternal dengan IAM Identity Center. Jika Anda berencana untuk menghubungkanAWS Managed Microsoft ADdirektori atau direktori yang dikelola sendiri di Active Directory, pastikan bahwa konfigurasi Active Directory Anda memenuhi prasyarat diActive Directory atau iDP eksternal.

> **Note**
>
> Sebagai praktik terbaik keamanan, kami sangat menyarankan Anda mengaktifkan otentikasi multi-faktor. Jika Anda berencana untuk menghubungkanAWS Managed Microsoft ADdirektori atau direktori yang dikelola sendiri di Active Directory dan Anda tidak menggunakan RADIUS MFAAWS Directory Service, aktifkan MFA di IAM Identity Center. Jika Anda berencana untuk menggunakan penyedia identitas eksternal, perhatikan bahwa IdP eksternal, bukan IAM Identity Center, mengelola pengaturan MFA. MFA di IAM Identity

Center tidak didukung untuk digunakan oleh eksternalIdPs. Untuk informasi lebih lanjut, lihatAktifkan MFAdi dalamAWS IAM Identity CenterPanduan Pengguna.

AWS Managed Microsoft AD

1. Tinjau pedoman diMenyambung ke Microsoft Active Directory.
2. Ikuti langkah-langkah diHubungkan direktori diAWS Managed Microsoft ADke IAM Identity Center.
3. Mengkonfigurasi Active Directory untuk menyinkronkan pengguna kepada siapa Anda ingin memberikan izin administratif ke IAM Identity Center. Untuk informasi lebih lanjut, lihatSinkronisasi pengguna administratif ke IAM Identity Center.

Direktori yang dikelola sendiri di Active Directory

1. Tinjau pedoman diMenyambung ke Microsoft Active Directory.
2. Ikuti langkah-langkah diMenghubungkan direktori yang dikelola sendiri di Active Directory ke IAM Identity Center.
3. Mengkonfigurasi Active Directory untuk menyinkronkan pengguna kepada siapa Anda ingin memberikan izin administratif ke IAM Identity Center. Untuk informasi lebih lanjut, lihatSinkronisasi pengguna administratif di IAM Identity Center.

IdP eksternal

1. Tinjau pedoman diTerhubung ke penyedia identitas eksternal.
2. Ikuti langkah-langkah diCara terhubung ke penyedia identitas eksternal.
3. Konfigurasikan IdP Anda untuk menyediakan pengguna ke IAM Identity Center.

> **Note**
>
> Sebelum menyiapkan penyediaan semua identitas tenaga kerja Anda secara otomatis dan berbasis grup dari IdP Anda ke IAM Identity Center, sebaiknya Anda menyinkronkan satu pengguna yang ingin Anda berikan izin administratif ke IAM Identity Center.

Sinkronisasi pengguna administratif ke IAM Identity Center

Setelah Anda menghubungkan direktori Anda ke IAM Identity Center, Anda dapat menentukan pengguna kepada siapa Anda ingin memberikan izin administratif, dan kemudian menyinkronkan pengguna tersebut dari direktori Anda ke IAM Identity Center.

1. BukaKonsol IAM Identity Center.
2. Pilih Pengaturan.
3. PadaPengaturanhalaman, pilihSumber identitastab, pilihAksi, dan kemudian pilihKelola Sinkronisasi.
4. PadaKelola Sinkronisasihalaman, pilihPenggunatab, dan kemudian pilihMenambahkan pengguna dan grup.
5. PadaPenggunatab, di bawahPengguna, masukkan nama pengguna yang tepat dan pilihMenambahkan.
6. Di bawahDitambahkan Pengguna dan Grup, lakukan hal berikut:
   a. Konfirmasikan bahwa pengguna yang ingin Anda berikan izin administratif ditentukan.
   b. Pilih kotak centang di sebelah kiri nama pengguna.
   c. Pilih Submit (Kirim).
7. DalamKelola sinkronisasihalaman, pengguna yang Anda tentukan muncul diPengguna dalam lingkup sinkronisasidaftar.
8. Di panel navigasi, pilih Users (Pengguna).
9. PadaPenggunahalaman, mungkin perlu beberapa waktu bagi pengguna yang Anda tentukan untuk muncul dalam daftar. Pilih ikon refresh untuk memperbarui daftar pengguna.

Pada titik ini, pengguna Anda tidak memiliki akses ke akun manajemen. Anda akan menyiapkan akses administratif ke akun ini dengan membuat set izin administratif dan menetapkan pengguna ke set izin tersebut.

Langkah selanjutnya: Langkah 3: Buat set izin administratif

Gunakan direktori default dan buat pengguna di IAM Identity Center

Saat Anda mengaktifkan IAM Identity Center untuk pertama kalinya, maka secara otomatis dikonfigurasi dengan direktori IAM Identity Center sebagai sumber identitas default Anda. Selesaikan langkah-langkah berikut untuk membuat pengguna di IAM Identity Center.

1. Masuk keAWS Management Consolesebagai pemilik akun dengan memilihPengguna rootdan memasukiAkun AWSalamat email. Di laman berikutnya, masukkan kata sandi Anda.
2. BukaKonsol IAM Identity Center.
3. Ikuti langkah-langkah diTambahkan penggunauntuk membuat pengguna.

   Saat Anda menentukan detail pengguna, Anda dapat mengirim email dengan instruksi pengaturan kata sandi (ini adalah opsi default) atau membuat kata sandi satu kali. Jika Anda mengirim email, pastikan Anda menentukan alamat email yang dapat Anda akses.
4. Setelah Anda menambahkan pengguna, kembali ke prosedur ini. Jika Anda menyimpan opsi default untuk mengirim email dengan instruksi pengaturan kata sandi, lakukan hal berikut:

   a. Anda akan menerima email dengan subjekUndangan untuk bergabungAWSSistem Masuk Tunggal. Buka email dan pilihTerima undangan.
   b. PadaPengguna baru mendaftarhalaman, masukkan dan konfirmasikan kata sandi, lalu pilihTetapkan kata sandi baru.

   > **Note**
   >
   > Pastikan untuk menyimpan kata sandi Anda. Anda akan membutuhkannya nanti untukLangkah 5: Masuk keAWSakses portal dengan kredensi administratif Anda.

Pada titik ini, pengguna Anda tidak memiliki akses ke akun manajemen. Anda akan menyiapkan akses administratif ke akun ini dengan membuat set izin administratif dan menetapkan pengguna ke set izin tersebut.

Langkah selanjutnya: Langkah 3: Buat set izin administratif

Langkah 3: Buat set izin administratif

Set izin disimpan di IAM Identity Center dan menentukan tingkat akses yang dimiliki pengguna dan grupAkun AWS. Lakukan langkah-langkah berikut untuk membuat set izin yang memberikan izin administratif.

1. Masuk keAWS Management Consolesebagai pemilik akun dengan memilihPengguna rootdan memasukiAkun AWSalamat email. Di laman berikutnya, masukkan kata sandi Anda.
2. BukaKonsol IAM Identity Center.

3. Di panel navigasi IAM Identity Center, di bawahIzin multi-akun, pilihSet izin.
4. PilihBuat set izin.
5. UntukLangkah 1: Pilih jenis set izin, padaPilih jenis set izinhalaman, menjaga pengaturan default dan memilihBerikutnya. Pengaturan default memberikan akses penuh keAWSlayanan dan sumber daya menggunakanAdministratorAccessset izin yang telah ditetapkan.

> **Note**
>
> Yang telah ditetapkanAdministratorAccessizin set menggunakanAdministratorAccess AWSkebijakan yang dikelola.

6. UntukLangkah 2: Tentukan rincian set izin, padaTentukan rincian set izinhalaman, menjaga pengaturan default dan memilihBerikutnya. Pengaturan default membatasi sesi Anda hingga satu jam.
7. UntukLangkah 3: Tinjau dan buat, padaTinjau dan buathalaman, lakukan hal berikut:
   1. Tinjau jenis set izin dan konfirmasikan bahwa ituAdministratorAccess.
   2. TinjauAWSkebijakan yang dikelola dan konfirmasikanAdministratorAccess.
   3. Pilih Buat.

Langkah 4: MengaturAkun AWSakses untuk pengguna administratif

Untuk mengaturAkun AWSakses untuk pengguna administratif di IAM Identity Center, Anda harus menetapkan pengguna keAdministratorAccessizin ditetapkan.

1. Masuk keAWS Management Consolesebagai pemilik akun dengan memilihPengguna rootdan memasukiAkun AWSalamat email. Di laman berikutnya, masukkan kata sandi Anda.
2. BukaKonsol IAM Identity Center.
3. Di panel navigasi, di bawahIzin multi-akun, pilihAkun AWS.
4. PadaAkun AWShalaman, daftar tampilan pohon organisasi Anda muncul. Pilih kotak centang di sampingAkun AWSyang ingin Anda tetapkan akses administratif. Jika Anda memiliki beberapa akun di organisasi, centang kotak di samping akun manajemen.
5. PilihMenetapkan pengguna atau grup.
6. UntukLangkah 1: Pilih pengguna dan grup, padaTetapkan pengguna dan grup ke”***AWS-nama akun***“halaman, lakukan hal berikut:

1. PadaPenggunatab, pilih pengguna kepada siapa Anda ingin memberikan izin administratif.

   Untuk memfilter hasil, mulailah mengetik nama pengguna yang Anda inginkan di kotak pencarian.

2. Setelah Anda mengonfirmasi bahwa pengguna yang benar dipilih, pilihBerikutnya.

7. UntukLangkah 2: Pilih set izin, padaTetapkan set izin ke"***AWS-nama akun***"halaman, di bawahSet izin, pilihAdministratorAccessizin ditetapkan.
8. Pilih Selanjutnya.
9. UntukLangkah 3: Tinjau dan Kirim, padaTinjau dan kirimkan tugas ke"***AWS-nama akun***"halaman, lakukan hal berikut:

   1. Tinjau set pengguna dan izin yang dipilih.
   2. Setelah Anda mengkonfirmasi bahwa pengguna yang benar ditugaskan keAdministratorAccessset izin, pilihMenyerahkan.

   > **Important**
   >
   > Proses penetapan pengguna mungkin memerlukan beberapa menit untuk menyelesaikannya. Biarkan halaman ini terbuka sampai proses berhasil diselesaikan.

10. Jika salah satu dari berikut ini berlaku, ikuti langkah-langkah diAktifkan MFAuntuk mengaktifkan MFA untuk IAM Identity Center:

    - Anda menggunakan direktori Pusat Identitas default sebagai sumber identitas Anda.
    - Anda menggunakanAWS Managed Microsoft ADdirektori atau direktori yang dikelola sendiri di Active Directory sebagai sumber identitas Anda dan Anda tidak menggunakan RADIUS MFA denganAWS Directory Service.

    > **Note**
    >
    > Jika Anda menggunakan penyedia identitas eksternal, perhatikan bahwa IdP eksternal, bukan IAM Identity Center, mengelola pengaturan MFA. MFA di IAM Identity Center tidak didukung untuk digunakan oleh eksternalIdPs.

Saat Anda menyiapkan akses akun untuk pengguna administratif, IAM Identity Center akan membuat peran IAM yang sesuai. Peran ini, yang dikendalikan oleh IAM Identity Center, dibuat dalam hal yang relevanAkun AWS, dan kebijakan yang ditentukan dalam kumpulan izin dilampirkan ke peran.

Langkah 5: Masuk keAWSakses portal dengan kredensi administratif Anda

Selesaikan langkah-langkah berikut untuk mengonfirmasi bahwa Anda dapat masuk keAWSakses portal dengan menggunakan kredensi pengguna administratif, dan bahwa Anda dapat mengaksesAkun AWS.

1. Masuk keAWS Management Consolesebagai pemilik akun dengan memilihPengguna rootdan memasukiAkun AWSalamat email. Di laman berikutnya, masukkan kata sandi Anda.
2. BukaAWS IAM Identity Centerkonsol dihttps://console.aws.amazon.com/singlesignon/.
3. Di panel navigasi, pilih Dasbor.
4. PadaDasborhalaman, di bawahRingkasan pengaturan, salinAWSakses URL portal.
5. Buka browser terpisah, tempelAWSakses URL portal yang Anda salin, dan tekanMemasukkan.
6. Masuk dengan menggunakan salah satu dari berikut ini:
   - Jika Anda menggunakan Active Directory atau penyedia identitas eksternal (IdP) sebagai sumber identitas Anda, masuk dengan menggunakan kredensi pengguna Active Directory atau IdP yang Anda tetapkan keAdministratorAccessizin diatur dalam IAM Identity Center.
   - Jika Anda menggunakan direktori IAM Identity Center default sebagai sumber identitas Anda, masuk dengan menggunakan nama pengguna yang Anda tentukan saat membuat pengguna dan kata sandi baru yang Anda tentukan untuk pengguna.
7. Setelah Anda masuk, sebuahAkun AWSikon muncul di portal.
8. Bila Anda memilihAkun AWSikon, nama akun, ID akun, dan alamat email yang terkait dengan akun muncul.
9. Pilih nama akun untuk menampilkanAdministratorAccessizin set, dan pilihKonsol Manajemenlink ke kananAdministratorAccess.

   Saat Anda masuk, nama set izin yang ditetapkan pengguna akan muncul sebagai peran yang tersedia diAWSportal akses. Karena Anda menetapkan pengguna ini keAdministratorAccessizin set, peran akan muncul diAWSportal akses sebagai:AdministratorAccess/*nama pengguna*

10. Jika Anda diarahkan keAWSManagement Console, Anda berhasil menyelesaikan pengaturan akses administratif keAkun AWS. Lanjutkan ke langkah 10.
11. Beralih ke browser yang Anda gunakan untuk masuk keAWS Management Consoledan mengatur IAM Identity Center, dan keluar dariAkun AWSpengguna root.

> **Important**
>
> Kami sangat menyarankan agar Anda mematuhi praktik terbaik dalam menggunakan kredensi pengguna administratif saat Anda masuk keAWSakses portal, dan bahwa Anda tidak menggunakan kredensi pengguna root untuk tugas sehari-hari Anda.

Untuk memungkinkan pengguna lain mengakses akun dan aplikasi Anda, dan mengelola IAM Identity Center, buat dan tetapkan set izin hanya melalui IAM Identity Center.

Pemecahan MasalahAkun AWSmasalah penciptaan

Gunakan informasi di sini untuk membantu Anda memecahkan masalah terkait pembuatanAkun AWS.

Masalah

- Saya tidak menerima telepon dariAWSuntuk memverifikasi akun baru saya
- Saya mendapatkan kesalahan tentang “jumlah maksimum upaya gagal” ketika saya mencoba untuk memverifikasi sayaAkun AWSmelalui telepon
- Sudah lebih dari 24 jam dan akun saya tidak diaktifkan

Saya tidak menerima telepon dariAWSuntuk memverifikasi akun baru saya

Saat Anda membuatAkun AWS, Anda harus memberikan nomor telepon di mana Anda dapat menerima pesan teks SMS atau panggilan suara. Anda menentukan metode mana yang akan digunakan untuk memverifikasi nomor.

Jika Anda tidak menerima pesan atau panggilan, verifikasi hal berikut:

- Anda memasukkan nomor telepon yang benar dan memilih kode negara yang benar selama proses pendaftaran.
- Jika Anda menggunakan ponsel, pastikan Anda memiliki sinyal seluler untuk menerima pesan teks atau panggilan SMS.
- Informasi yang Anda masukkan untuk Andametode pembayaranbenar.

Jika Anda tidak menerima SMS atau panggilan untuk menyelesaikan proses verifikasi identitas,AWS Supportdapat membantu Anda mengaktifkanAkun AWSsecara manual. Gunakan langkah-langkah berikut:

1. Pastikan bahwa Anda dapat dihubungi dinomor teleponyang Anda berikan untuk AndaAkun AWS.
2. BukaAWS Supportkonsol, lalu pilihBuat kasus.
   a. Pilih Support akun dan penagihan.
   b. UntukJenis, pilihAkun.

c. UntukKategori, pilihAktivasi.
d. DalamDeskripsi kasusbagian, berikan tanggal dan waktu ketika Anda dapat dihubungi.
e. DalamOpsi kontakbagian, pilihobrolanuntukMetode kontak.
f. Pilih Submit (Kirim).

> **Note**
> Anda dapat membuat kasus denganAWS Supportbahkan jika AndaAkun AWStidak diaktifkan.

Saya mendapatkan kesalahan tentang “jumlah maksimum upaya gagal” ketika saya mencoba untuk memverifikasi sayaAkun AWSmelalui telepon

AWS Supportdapat membantu Anda mengaktifkan akun secara manual. Ikuti langkah-langkah ini:

1. Masuk keAkun AWSmenggunakan alamat email dan kata sandi yang Anda tentukan saat membuat akun Anda.
2. BukaAWS Supportkonsol, lalu pilihBuat kasus.
3. PilihDukungan Akun dan Penagihan.
4. UntukJenis, pilihAkun.
5. UntukKategori, pilihAktivasi.
6. DalamDeskripsi kasusbagian, berikan tanggal dan waktu ketika Anda dapat dihubungi.
7. DalamOpsi kontakbagian, pilihobrolanuntukMetode kontak.
8. Pilih Submit (Kirim).

AWS Supportakan menghubungi Anda dan mencoba untuk secara manual mengaktifkan AndaAkun AWS.

Sudah lebih dari 24 jam dan akun saya tidak diaktifkan

Aktivasi akun terkadang dapat ditunda. Jika prosesnya memakan waktu lebih dari 24 jam, periksa hal berikut:

- Selesaikan proses aktivasi akun.

  Jika Anda menutup jendela untuk proses pendaftaran sebelum Anda menambahkan semua informasi yang diperlukan, bukaregistrasihalaman. PilihMasuk ke yang sudah adaAkun AWS, dan masuk menggunakan alamat email dan kata sandi yang Anda pilih untuk akun tersebut.
- Periksa informasi yang terkait dengan metode pembayaran Anda.

  DalamAWS Billing and Cost Managementkonsol, periksaMetode Pembayaranuntuk kesalahan.
- Hubungi lembaga keuangan Anda.

  Terkadang lembaga keuangan menolak permintaan otorisasi dariAWS. Hubungi institusi yang terkait dengan metode pembayaran Anda, dan minta mereka untuk menyetujui permintaan otorisasi dariAWS.AWSmembatalkan permintaan otorisasi segera setelah disetujui oleh lembaga keuangan Anda, sehingga Anda tidak dikenakan biaya untuk permintaan otorisasi. Permintaan otorisasi mungkin masih muncul sebagai biaya kecil (biasanya 1 USD) pada laporan dari lembaga keuangan Anda.
- Periksa email dan folder spam Anda untuk meminta informasi tambahan.
- Coba browser yang berbeda.
- KontakAWS Support.

  KontakAWS Supportuntuk bantuan. Sebutkan langkah-langkah pemecahan masalah yang sudah Anda coba.

> **Note**
>
> Jangan memberikan informasi sensitif, seperti nomor kartu kredit, dalam korespondensi apa pun denganAWS.

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