Panduan Pengguna

AWS Pengaturan

AWS Pengaturan: Panduan Pengguna

Table of Contents

Gambaran Umum

Panduan ini memberikan petunjuk untuk membuat pengguna baru Akun AWS dan mengatur pengguna administratif pertama Anda dalam AWS IAM Identity Center mengikuti praktik terbaik keamanan terbaru.

An Akun AWS diperlukan untuk mengakses Layanan AWS dan berfungsi sebagai dua fungsi dasar:

- Kontainer — An Akun AWS adalah wadah untuk semua AWS sumber daya yang dapat Anda buat sebagai AWS pelanggan. Saat membuat bucket Amazon Simple Storage Service (Amazon S3) atau database Amazon Relational Database Service (Amazon RDS) untuk menyimpan data, atau instans Amazon Elastic Compute Cloud EC2 (Amazon) untuk memproses data, Anda membuat sumber daya di akun Anda. 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 — An Akun AWS adalah batas keamanan dasar untuk sumber daya Anda. AWS Sumber daya yang Anda buat di akun hanya tersedia untuk pengguna yang memiliki kredensi untuk akun yang sama.

  Di antara sumber daya utama yang dapat Anda buat di akun Anda adalah identitas, seperti pengguna dan peran IAM, dan identitas gabungan, seperti pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas IAM, atau pengguna lain yang mengakses Layanan AWS dengan menggunakan kredensi yang disediakan melalui sumber identitas. Identitas ini memiliki kredensi yang dapat digunakan seseorang untuk masuk, atau mengautentikasi. AWS Identitas juga memiliki kebijakan izin yang menentukan apa yang diizinkan oleh orang yang masuk 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 mengawasi Akun AWS. Administrator memiliki tingkat izin yang lebih tinggi Akun AWS daripada anggota lain dari organisasi mereka. Administrator menetapkan dan menerapkan 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. Dalam AWS, 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 profil Akun 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.

AWS pengguna dan kredensialnya

Saat berinteraksi AWS, Anda menentukan kredensi AWS keamanan untuk memverifikasi siapa Anda dan apakah Anda memiliki izin untuk mengakses sumber daya yang Anda minta. AWS menggunakan 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 Anda AWS . 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 Anda Akun AWS. Saat pertama kali membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. 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 membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam 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 Anda Akun 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 gabungan

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).

AWS Pengguna 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. AWS Builder ID mewakili Anda sebagai pribadi, dan Anda dapat menggunakannya untuk mengakses AWS layanan dan alat tanpa Akun 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 satu Akun AWS, dan pahami persyaratan untuk menyiapkan akun Anda untuk akses administratif di Pusat Identitas IAM.

Akun AWS persyaratan

Untuk mendaftar Akun AWS, Anda perlu memberikan informasi berikut:

- 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 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 seperti organisasi - tujuan - lingkungan (misalnya, AnyCompany- audit - prod). Jika itu adalah akun pribadi, pertimbangkan untuk menggunakan standar penamaan seperti nama depan - nama belakang - tujuan (misalnya, paulo-santos-testaccount).
- Alamat email — Alamat email ini digunakan sebagai nama masuk 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 mengakses Akun AWS jika 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 ketika 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 mengakses Akun AWS jika seorang karyawan mengubah posisi atau meninggalkan perusahaan.

- Perangkat otentikasi multi-faktor — Untuk mengamankan AWS sumber daya Anda, aktifkan otentikasi multi-faktor (MFA) pada akun pengguna root. Selain kredensi masuk reguler Anda, otentikasi sekunder diperlukan saat MFA diaktifkan, memberikan lapisan keamanan tambahan. Untuk informasi lebih lanjut tentang MFA, lihat Apa itu MFA? di Panduan Pengguna IAM.
- Dukungan rencana — Anda akan diminta untuk memilih salah satu paket yang tersedia selama proses pembuatan akun. Untuk deskripsi paket yang tersedia, lihat Membandingkan Dukungan paket.

Pertimbangan IAM Identity Center

Topik berikut memberikan panduan untuk menyiapkan Pusat Identitas IAM untuk lingkungan tertentu. Pahami panduan yang berlaku untuk lingkungan Anda sebelum Anda melanjutkan keBagian 2: Buat pengguna administratif di IAM Identity Center.

Topik

- Direktori Aktif atau iDP eksternal
- AWS Organizations
- Peran IAM
- Firewall generasi berikutnya dan gateway web yang aman

Direktori Aktif 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 mengaktifkan IAM Identity Center dan memilih sumber identitas Anda. Melakukan hal ini sebelum Anda membuat pengguna dan grup 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 menggunakan AWS Managed Microsoft AD, Anda harus mengaktifkan IAM Identity Center di tempat yang sama Wilayah AWS di mana AWS Managed Microsoft AD direktori Anda diatur. IAM Identity Center menyimpan data penugasan di Wilayah yang sama dengan direktori. Untuk mengelola Pusat Identitas IAM, Anda mungkin perlu beralih ke Wilayah tempat Pusat Identitas IAM dikonfigurasi. Juga, perhatikan bahwa portal AWS akses menggunakan URL akses yang sama dengan direktori Anda.
- Gunakan Active Directory yang berada di akun manajemen Anda:

  Anda harus memiliki AD Connector atau AWS Managed Microsoft AD direktori yang sudah ada AWS Directory Service, dan direktori tersebut harus berada di dalam akun AWS Organizations manajemen Anda. Anda hanya dapat menghubungkan satu AD Connector atau satu AWS Managed Microsoft AD per satu. Jika Anda perlu mendukung beberapa domain atau hutan, gunakan AWS Managed Microsoft AD. Untuk informasi selengkapnya, lihat:

  - Hubungkan direktori AWS Managed Microsoft AD ke Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.
  - Hubungkan direktori yang dikelola sendiri di Active Directory ke IAM Identity Center di AWS IAM Identity Center Panduan 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 AD Connector atau AWS Managed Microsoft AD direktori yang sudah ada yang disiapkan di AWS direktori 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 berada di akun manajemen.

AWS Organizations

Anda Akun AWS harus dikelola oleh AWS Organizations. Jika Anda belum mendirikan organisasi, Anda tidak perlu melakukannya. Ketika Anda mengaktifkan IAM Identity Center, Anda akan memilih apakah akan AWS membuat organisasi untuk Anda.

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

Untuk mengaktifkan Pusat Identitas IAM, Anda harus masuk ke AWS Management Console dengan menggunakan kredensyal akun manajemen Anda AWS Organizations . Anda tidak dapat mengaktifkan Pusat Identitas IAM saat masuk dengan kredensyal dari akun AWS Organizations anggota. Untuk informasi selengkapnya, lihat Membuat dan mengelola AWS Organisasi di Panduan AWS Organizations Pengguna.

Peran IAM

Jika Anda sudah mengonfigurasi peran IAM Akun AWS, kami sarankan Anda memeriksa apakah akun Anda mendekati kuota untuk peran IAM. Untuk informasi selengkapnya, lihat kuota objek IAM.

Jika Anda mendekati kuota, pertimbangkan untuk meminta kenaikan kuota. Jika tidak, Anda mungkin mengalami masalah dengan Pusat Identitas IAM saat Anda memberikan set izin ke akun yang telah melebihi kuota peran IAM. Untuk informasi tentang cara meminta kenaikan kuota, lihat Meminta kenaikan kuota pada Panduan Pengguna Service Quotas.

Firewall generasi berikutnya dan gateway web yang aman

Jika Anda memfilter akses ke AWS domain atau titik akhir URL tertentu dengan menggunakan solusi pemfilteran konten web seperti NGFWs atau SWGs, Anda harus menambahkan domain atau titik akhir URL berikut ke daftar izin solusi pemfilteran konten web Anda.

Domain DNS tertentu

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

Titik akhir URL tertentu

- https://.awsapps.com/mulai *[yourdirectory]*
- https://.awsapps.com/login *[yourdirectory]*
- https://*[yourregion]*.signin. aws/platform/login

Menggunakan beberapa Akun AWS

Akun AWS berfungsi sebagai batas keamanan mendasar di. AWS 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 diatur dengan baik.

Memisahkan sumber daya Anda 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 yang memerlukan kebijakan dan mekanisme kontrol yang berbeda. Misalnya, 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).
- Isolasi — An Akun AWS adalah unit perlindungan keamanan. Potensi risiko dan ancaman keamanan harus terkandung dalam sebuah 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 memindahkan mereka untuk memisahkan 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 mematuhi Peraturan Perlindungan Data Umum (GDPR) Uni Eropa.
- 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 menggabungkan tagihan) sambil memisahkan item baris. Akun AWS
- Alokasi kuota — kuota AWS layanan diberlakukan secara terpisah untuk masing-masing. Akun AWS Memisahkan beban kerja menjadi berbeda Akun AWS mencegah mereka dari mengkonsumsi kuota untuk satu sama lain.

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

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

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

Bagian 1: Siapkan yang baru Akun AWS

Instruksi ini akan membantu Anda membuat Akun AWS dan mengamankan kredensi pengguna root. Selesaikan semua langkah sebelum melanjutkan keBagian 2: Buat pengguna administratif di IAM Identity Center.

Topik

- Langkah 1: Mendaftar untuk AWS akun
- Langkah 2: Masuk sebagai pengguna root
- Langkah 3: Aktifkan MFA untuk pengguna root Anda Akun AWS

Langkah 1: Mendaftar untuk AWS akun

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Pilih Buat sebuah Akun AWS.

   > **Note**
   >
   > Jika Anda masuk AWS baru-baru ini, pilih Masuk ke Konsol. Jika opsi Buat baru Akun AWS tidak terlihat, pertama-tama pilih Masuk ke akun lain, lalu pilih Buat yang baru Akun AWS.

3. Masukkan informasi akun Anda, lalu pilih Lanjutkan.

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

4. Pilih Pribadi atau Profesional.

   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 AWS persyaratan.
6. Baca dan terima Perjanjian AWS Pelanggan.
7. Pilih Buat Akun dan Lanjutkan.

Pada titik ini, Anda akan menerima pesan email untuk mengonfirmasi bahwa Anda Akun AWS siap digunakan. Anda dapat masuk ke akun baru Anda dengan menggunakan alamat email dan kata sandi yang Anda berikan saat mendaftar. Namun, Anda tidak dapat menggunakan AWS layanan apa pun sampai Anda selesai mengaktifkan akun Anda.

8. Pada halaman Informasi Pembayaran, masukkan informasi tentang metode pembayaran Anda. Jika Anda ingin menggunakan alamat yang berbeda dari yang Anda gunakan untuk membuat akun, pilih Gunakan alamat baru dan masukkan alamat yang ingin Anda gunakan untuk tujuan penagihan.
9. Pilih Verifikasi dan Tambah.

> **Note**
>
> Jika alamat kontak Anda berada di India, perjanjian pengguna Anda untuk akun Anda adalah dengan AISPL, 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. AISPL membebankan 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 ke depan. Masukkan kode CAPTCHA, dan kirimkan.
11. Sistem verifikasi AWS otomatis memanggil Anda dan menyediakan PIN. Masukkan PIN menggunakan ponsel Anda dan kemudian pilih Lanjutkan.
12. Pilih Dukungan rencana.

    Untuk deskripsi paket yang tersedia, lihat Membandingkan Dukungan paket.

    Halaman konfirmasi muncul yang menunjukkan bahwa akun Anda sedang diaktifkan. Ini biasanya hanya memakan waktu beberapa menit tetapi kadang-kadang bisa memakan waktu hingga 24 jam. Selama aktivasi, Anda dapat masuk ke yang baru Akun AWS. Sampai aktivasi selesai, Anda mungkin melihat tombol Daftar Lengkap. Anda dapat mengabaikannya.

    AWS mengirimkan pesan email konfirmasi ketika aktivasi akun selesai. Periksa email dan folder spam Anda untuk pesan email konfirmasi. Setelah Anda menerima pesan ini, Anda memiliki akses penuh ke semua AWS layanan.

Langkah 2: Masuk sebagai pengguna root

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

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

Untuk masuk sebagai pengguna root

1. Buka 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 file Akun 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 untuk pengguna root Anda Akun AWS

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

Untuk petunjuk tentang mengaktifkan MFA untuk pengguna root, lihat Mengaktifkan perangkat MFA untuk pengguna AWS di Panduan Pengguna IAM.

Bagian 2: Buat pengguna administratif di IAM Identity Center

Setelah selesaiBagian 1: Siapkan yang baru Akun AWS, langkah-langkah berikut akan membantu Anda mengatur Akun AWS akses 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 untuk Akun AWS dan membuat pengguna administratif di Pusat Identitas IAM. Untuk informasi tambahan, lihat Memulai di Panduan AWS IAM Identity Center Pengguna.

Topik

Langkah 1: Aktifkan Pusat Identitas IAM

> **Note**
>
> Jika Anda tidak mengaktifkan otentikasi multi-faktor (MFA) untuk pengguna root Anda, selesaikan Langkah 3: Aktifkan MFA untuk pengguna root Anda Akun AWS sebelum Anda melanjutkan.

Untuk mengaktifkan Pusat Identitas IAM

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

2. Buka konsol Pusat Identitas IAM.
3. Di bawah Aktifkan Pusat Identitas IAM, pilih Aktifkan.
4. Pusat Identitas IAM membutuhkan AWS Organizations. Jika Anda belum membuat organisasi, Anda harus memilih apakah akan AWS membuat satu untuk Anda. Pilih Buat AWS organisasi untuk menyelesaikan proses ini.

   AWS Organizations secara 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, kami sarankan Anda mengonfigurasi administrasi yang didelegasikan. Dengan administrasi yang didelegasikan, Anda dapat membatasi jumlah orang yang memerlukan akses ke akun manajemen di AWS Organizations. Untuk informasi selengkapnya, lihat Administrasi Delegasi di Panduan AWS IAM Identity Center Pengguna.

Langkah 2: Pilih sumber identitas Anda

Sumber identitas Anda di IAM Identity Center menentukan di mana pengguna dan grup Anda dikelola. Anda dapat memilih salah satu dari berikut ini 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 serta menetapkan tingkat akses mereka ke akun dan aplikasi AWS Anda.
- Active Directory — Pilih opsi ini jika Anda ingin terus mengelola pengguna di direktori AWS Managed Microsoft AD Anda 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 Pusat Identitas IAM, Anda harus memilih sumber identitas Anda. Sumber identitas yang Anda pilih menentukan lokasi 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 untuk Anda. Akun AWS

> **Important**
>
> Jika Anda sudah mengelola pengguna dan grup di Active Directory atau penyedia identitas eksternal (iDP), sebaiknya Anda mempertimbangkan untuk menghubungkan sumber identitas ini saat 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 penetapan pengguna dan grup yang Anda konfigurasikan di Pusat Identitas IAM. Jika ini terjadi, semua pengguna, termasuk pengguna administratif di IAM Identity Center, akan kehilangan akses masuk tunggal ke aplikasi dan aplikasi mereka Akun AWS .

Topik

Connect 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 menghubungkan AWS Managed Microsoft AD direktori, direktori yang dikelola sendiri di Active Directory, atau iDP eksternal dengan IAM Identity Center. Jika Anda berencana untuk menghubungkan AWS Managed Microsoft AD direktori atau direktori yang dikelola sendiri di Active Directory, pastikan konfigurasi Active Directory Anda memenuhi prasyarat di. Direktori Aktif atau iDP eksternal

> **Note**
>
> Sebagai praktik keamanan terbaik, kami sangat menyarankan Anda mengaktifkan otentikasi multi-faktor. Jika Anda berencana untuk menghubungkan AWS Managed Microsoft AD direktori atau direktori yang dikelola sendiri di Active Directory dan Anda tidak menggunakan

RADIUS MFA, aktifkan MFA di AWS Directory Service IAM Identity Center. Jika Anda berencana untuk menggunakan penyedia identitas eksternal, perhatikan bahwa IDP eksternal, bukan Pusat Identitas IAM, mengelola pengaturan MFA. MFA di Pusat Identitas IAM tidak didukung untuk digunakan oleh eksternal. IdPs Untuk informasi selengkapnya, lihat Mengaktifkan MFA di AWS IAM Identity Center Panduan Pengguna.

AWS Managed Microsoft AD

1. Tinjau panduan di Connect to a Microsoft Active Directory.
2. Ikuti langkah-langkah di Connect direktori AWS Managed Microsoft AD ke IAM Identity Center.
3. Konfigurasikan Active Directory untuk menyinkronkan pengguna yang ingin Anda berikan izin administratif ke IAM Identity Center. Untuk informasi selengkapnya, lihat Menyinkronkan pengguna administratif ke Pusat Identitas IAM.

Direktori yang dikelola sendiri di Direktori Aktif

1. Tinjau panduan di Connect to a Microsoft Active Directory.
2. Ikuti langkah-langkah di Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center.
3. Konfigurasikan Active Directory untuk menyinkronkan pengguna yang ingin Anda berikan izin administratif ke IAM Identity Center. Untuk informasi selengkapnya, lihat Menyinkronkan pengguna administratif di Pusat Identitas IAM.

IDP Eksternal

1. Tinjau panduan di Connect ke penyedia identitas eksternal.
2. Ikuti langkah-langkah di Cara menyambung ke penyedia identitas eksternal.
3. Konfigurasikan IDP Anda untuk menyediakan pengguna ke Pusat Identitas IAM.

> **Note**
>
> Sebelum Anda mengatur penyediaan otomatis berbasis grup dari semua identitas tenaga kerja Anda dari IDP Anda ke IAM Identity Center, kami sarankan 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 yang ingin Anda berikan izin administratif, dan kemudian menyinkronkan pengguna tersebut dari direktori Anda ke Pusat Identitas IAM.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Pada halaman Kelola Sinkronisasi, pilih tab Pengguna, lalu pilih Tambahkan pengguna dan grup.
5. Pada tab Pengguna, di bawah Pengguna, masukkan nama pengguna yang tepat dan pilih Tambah.
6. Di bawah Pengguna dan Grup yang Ditambahkan, 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 Kirim.
7. Di halaman Kelola sinkronisasi, pengguna yang Anda tentukan muncul di daftar cakupan pengguna dalam sinkronisasi.
8. Di panel navigasi, pilih Pengguna.
9. Pada halaman Pengguna, mungkin diperlukan beberapa waktu bagi pengguna yang Anda tentukan untuk muncul dalam daftar. Pilih ikon penyegaran untuk memperbarui daftar pengguna.

Pada titik ini, pengguna Anda tidak memiliki akses ke akun manajemen. Anda akan mengatur 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

Ketika Anda mengaktifkan IAM Identity Center untuk pertama kalinya, 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 ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
2. Buka konsol Pusat Identitas IAM.
3. Ikuti langkah-langkah di Tambahkan pengguna untuk 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 subjek Undangan untuk bergabung dengan AWS Single Sign-On. Buka email dan pilih Terima undangan.

   b. Pada halaman pendaftaran pengguna baru, masukkan dan konfirmasikan kata sandi, lalu pilih Tetapkan kata sandi baru.

   > **Note**
   >
   > Pastikan untuk menyimpan kata sandi Anda. Anda akan membutuhkannya nantiLangkah 5: Masuk ke portal AWS akses dengan kredensi administratif Anda.

Pada titik ini, pengguna Anda tidak memiliki akses ke akun manajemen. Anda akan mengatur 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 Pusat Identitas IAM dan menentukan tingkat akses yang dimiliki pengguna dan grup ke. Akun AWS Lakukan langkah-langkah berikut untuk membuat set izin yang memberikan izin administratif.

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
2. Buka konsol Pusat Identitas IAM.

3. Di panel navigasi Pusat Identitas IAM, di bawah izin Multi-akun, pilih Set izin.
4. Pilih Buat set izin.
5. Untuk Langkah 1: Pilih jenis set izin, pada halaman Pilih jenis set izin, pertahankan pengaturan default dan pilih Berikutnya. Pengaturan default memberikan akses penuh ke AWS layanan dan sumber daya menggunakan set izin yang AdministratorAccesstelah ditentukan sebelumnya.

   > **Note**
   >
   > Set AdministratorAccessizin yang telah ditentukan menggunakan kebijakan AdministratorAccess AWS terkelola.

6. Untuk Langkah 2: Tentukan detail set izin, pada halaman Tentukan detail set izin, pertahankan pengaturan default dan pilih Berikutnya. Pengaturan default membatasi sesi Anda menjadi satu jam.
7. Untuk Langkah 3: Tinjau dan buat, pada halaman Tinjau dan buat, lakukan hal berikut:

   1. Tinjau jenis set izin dan konfirmasikan bahwa itu benar AdministratorAccess.
   2. Tinjau kebijakan yang AWS dikelola dan konfirmasikan bahwa itu benar AdministratorAccess.
   3. Pilih Buat.

Langkah 4: Siapkan Akun AWS akses untuk pengguna administratif

Untuk mengatur Akun AWS akses bagi pengguna administratif di Pusat Identitas IAM, Anda harus menetapkan pengguna ke set AdministratorAccessizin.

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
2. Buka konsol Pusat Identitas IAM.
3. Di panel navigasi, di bawah Izin multi-akun, pilih. Akun AWS
4. Pada Akun AWShalaman, daftar tampilan pohon organisasi Anda akan muncul. Pilih kotak centang di sebelah yang Akun AWS ingin Anda tetapkan akses administratif. Jika Anda memiliki beberapa akun di organisasi Anda, pilih kotak centang di sebelah akun manajemen.
5. Pilih Tetapkan pengguna atau grup.
6. Untuk Langkah 1: Pilih pengguna dan grup, pada halaman Tetapkan pengguna dan grup ke ***AWS-account-name*** "", lakukan hal berikut:

1. Pada tab Pengguna, pilih pengguna yang ingin Anda berikan izin administratif.

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

2. Setelah Anda mengonfirmasi bahwa pengguna yang benar dipilih, pilih Berikutnya.

7. Untuk Langkah 2: Pilih set izin, pada halaman Tetapkan set izin ke ***AWS-account-name*** "", di bawah Set izin, pilih set AdministratorAccessizin.
8. Pilih Berikutnya.
9. Untuk Langkah 3: Tinjau dan Kirim, pada Review dan kirimkan tugas ke halaman ***AWS-account-name*** "", lakukan hal berikut:

   1. Tinjau pengguna yang dipilih dan set izin.
   2. Setelah Anda mengonfirmasi bahwa pengguna yang benar ditetapkan ke set AdministratorAccessizin, pilih Kirim.

   > **Important**
   >
   > Proses penugasan pengguna mungkin membutuhkan waktu beberapa menit untuk diselesaikan. Biarkan halaman ini terbuka sampai proses berhasil diselesaikan.

10. Jika salah satu dari berikut ini berlaku, ikuti langkah-langkah di Aktifkan MFA untuk mengaktifkan MFA untuk Pusat Identitas IAM:

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

    > **Note**
    >
    > Jika Anda menggunakan penyedia identitas eksternal, perhatikan bahwa iDP eksternal, bukan Pusat Identitas IAM, mengelola pengaturan MFA. MFA di Pusat Identitas IAM tidak didukung untuk digunakan oleh eksternal. IdPs

Saat Anda mengatur akses akun untuk pengguna administratif, Pusat Identitas IAM akan membuat peran IAM yang sesuai. Peran ini, yang dikendalikan oleh Pusat Identitas IAM, dibuat dalam peran yang relevan Akun AWS, dan kebijakan yang ditentukan dalam kumpulan izin dilampirkan ke peran.

Langkah 5: Masuk ke portal AWS akses dengan kredensi administratif Anda

Selesaikan langkah-langkah berikut untuk mengonfirmasi bahwa Anda dapat masuk ke portal AWS akses dengan menggunakan kredensi pengguna administratif, dan bahwa Anda dapat mengakses. Akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
2. Buka AWS IAM Identity Center konsol di https://console.aws.amazon.com/singlesignon/.
3. Di panel navigasi, pilih Dasbor.
4. Pada halaman Dasbor, di bawah Ringkasan pengaturan, salin URL portal AWS akses.
5. Buka browser terpisah, tempel URL portal AWS akses yang Anda salin, dan tekan Enter.
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 kredenal Active Directory atau pengguna iDP yang Anda tetapkan ke AdministratorAccessizin yang ditetapkan di IAM Identity Center.
   - Jika Anda menggunakan direktori IAM Identity Center default sebagai sumber identitas Anda, masuk dengan menggunakan nama pengguna yang Anda tentukan saat Anda membuat pengguna dan kata sandi baru yang Anda tentukan untuk pengguna.
7. Setelah Anda masuk, Akun AWSikon muncul di portal.
8. Saat Anda memilih Akun AWSikon, nama akun, ID akun, dan alamat email yang terkait dengan akun akan muncul.
9. Pilih nama akun untuk menampilkan set AdministratorAccessizin, dan pilih tautan Management Console di sebelah kanan AdministratorAccess.

   Saat Anda masuk, nama izin yang disetel ke mana pengguna ditetapkan muncul sebagai peran yang tersedia di portal AWS akses. Karena Anda menetapkan pengguna

ini ke set `AdministratorAccess` izin, peran akan muncul di portal AWS akses sebagai:`AdministratorAccess/`*`username`*

10. Jika Anda dialihkan ke Konsol AWS Manajemen, Anda berhasil menyelesaikan pengaturan akses administratif ke Akun AWS. Lanjutkan ke langkah 10.
11. Beralih ke browser yang Anda gunakan untuk masuk ke AWS Management Console dan mengatur Pusat Identitas IAM, dan keluar dari pengguna Akun AWS root Anda.

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

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

Memecahkan masalah pembuatan Akun AWS

Gunakan informasi di sini untuk membantu Anda memecahkan masalah yang terkait dengan pembuatan file. Akun AWS

Masalah

- Saya tidak menerima panggilan dari AWS untuk memverifikasi akun baru saya
- Saya mendapatkan kesalahan tentang “jumlah maksimum upaya yang gagal” ketika saya mencoba memverifikasi Akun AWS melalui telepon
- Sudah lebih dari 24 jam dan akun saya tidak diaktifkan

Saya tidak menerima panggilan dari AWS untuk memverifikasi akun baru saya

Saat Anda membuat Akun AWS, Anda harus memberikan nomor telepon tempat 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 metode pembayaran Anda benar.

Jika Anda tidak menerima pesan teks SMS atau panggilan untuk menyelesaikan proses verifikasi identitas, Dukungan dapat membantu Anda untuk mengaktifkan Akun AWS secara manual. Gunakan langkah-langkah berikut:

1. Pastikan Anda dapat dihubungi di nomor telepon yang Anda berikan untuk Anda Akun AWS.
2. Buka AWS Dukungan konsol, lalu pilih Buat kasus.
   a. Pilih Support akun dan penagihan.
   b. Untuk Jenis, pilih Akun.

c. Untuk Kategori, pilih Aktivasi.
d. Di bagian Deskripsi kasus, berikan tanggal dan waktu kapan Anda dapat dihubungi.
e. Di bagian Opsi kontak, pilih Metode Obrolan untuk Kontak.
f. Pilih Kirim.

> **Note**
>
> Anda dapat membuat kasus dengan Dukungan bahkan jika Anda Akun AWS tidak diaktifkan.

Saya mendapatkan kesalahan tentang “jumlah maksimum upaya yang gagal” ketika saya mencoba memverifikasi Akun AWS melalui telepon

Dukungan dapat membantu Anda mengaktifkan akun Anda secara manual. Ikuti langkah-langkah ini:

1. Masuk ke Anda Akun AWS menggunakan alamat email dan kata sandi yang Anda tentukan saat membuat akun.
2. Buka Dukungan konsol, lalu pilih Buat kasus.
3. Pilih Akun dan Dukungan Penagihan.
4. Untuk Jenis, pilih Akun.
5. Untuk Kategori, pilih Aktivasi.
6. Di bagian Deskripsi kasus, berikan tanggal dan waktu kapan Anda dapat dihubungi.
7. Di bagian Opsi kontak, pilih Metode Obrolan untuk Kontak.
8. Pilih Kirim.

Dukungan akan menghubungi Anda dan mencoba untuk mengaktifkan Anda secara manual Akun 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, buka halaman pendaftaran. Pilih Masuk ke yang sudah ada Akun AWS, dan masuk menggunakan alamat email dan kata sandi yang Anda pilih untuk akun tersebut.
- Periksa informasi yang terkait dengan metode pembayaran Anda.

  Di AWS Manajemen Penagihan dan Biaya konsol, periksa Metode Pembayaran untuk kesalahan.
- Hubungi lembaga keuangan Anda.

  Terkadang lembaga keuangan menolak permintaan otorisasi dari. AWS Hubungi lembaga yang terkait dengan metode pembayaran Anda, dan minta mereka untuk menyetujui permintaan otorisasi dari. AWS AWS membatalkan 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 folder email dan spam Anda untuk permintaan informasi tambahan.
- Coba browser yang berbeda.
- Kontak AWS Dukungan.

  Hubungi AWS Dukunganuntuk bantuan. Sebutkan langkah-langkah pemecahan masalah yang sudah Anda coba.

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

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