aws

Panduan Memulai

# Konsol Manajemen AWS

Versi 1.0

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

# Konsol Manajemen AWS: Panduan Memulai

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

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

# Table of Contents

Apa itu Konsol Manajemen AWS? ..... 1
Fitur Konsol Manajemen AWS ..... 1
AWS Konsol layanan individu ..... 2
Mengakses Konsol Manajemen AWS ..... 2
Mengakses Konsol Manajemen AWS dengan perangkat seluler ..... 2
Memulai dengan layanan ..... 4
Navigasi Terpadu ..... 5
Mengakses menu Layanan ..... 5
Mencari produk, layanan, fitur, dan lainnya ..... 6
Mencari AWS produk ..... 7
Menyempurnakan pencarian Anda ..... 7
Melihat fitur layanan ..... 8
Peluncuran AWS CloudShell ..... 8
Mengakses AWS notifikasi dan acara Kesehatan ..... 9
Mendapatkan Dukungan ..... 9
Mengkonfigurasi Konsol Manajemen AWS ..... 10
Mengkonfigurasi Pengaturan Terpadu ..... 10
Mengkonfigurasi Wilayah dan layanan yang terlihat ..... 13
Memilih Wilayah Anda ..... 15
Favorit ..... 17
Mengubah kata sandi ..... 22
Mengubah bahasa Konsol Manajemen AWS ..... 24
Mengakses informasi Anda AWS ..... 26
Mengakses informasi akun ..... 27
Mengakses informasi organisasi ..... 27
Mengakses informasi kuota layanan ..... 28
Mengakses informasi penagihan ..... 28
Masuk ke beberapa akun ..... 28
Menggunakan tindakan yang disarankan ..... 29
Fitur Tindakan yang AWS Direkomendasikan ..... 30
Menggunakan tindakan yang disarankan ..... 30
Pemantauan dengan CloudTrail log ..... 31
AWS Console Home ..... 34
Melihat semua AWS layanan ..... 34

Bekerja dengan Widget ... 34
Mengelola widget ... 35
MyApplications ... 36
Fitur MyApplications ... 37
Layanan terkait ... 37
Mengakses MyApplications ... 38
Harga ... 38
Wilayah yang Didukung ... 38
Aplikasi ... 39
Sumber daya ... 48
Dasbor myApplications ... 52
Mengobrol dengan Amazon Q ... 56
Memulai Amazon Q ... 56
Contoh pertanyaan ... 56
Konsol Manajemen AWS Akses Pribadi ... 58
Didukung Wilayah AWS, konsol layanan, dan fitur ... 58
Ikhtisar kontrol keamanan Akses Konsol Manajemen AWS Pribadi ... 64
Pembatasan akun Konsol Manajemen AWS dari jaringan Anda ... 64
Konektivitas dari jaringan Anda ke internet ... 64
Titik akhir VPC dan konfigurasi DNS yang diperlukan ... 64
DNSkonfigurasi ... 65
Titik akhir dan konfigurasi VPC untuk layanan DNS AWS ... 67
Menerapkan kebijakan kontrol layanan dan kebijakan titik akhir VPC ... 69
Kebijakan kontrol layanan ... 69
Kebijakan VPC endpoint ... 70
Menerapkan kebijakan berbasis identitas dan jenis kebijakan lainnya ... 72
Kunci konteks kondisi AWS global yang didukung ... 72
Bagaimana Konsol Manajemen AWS Private Access bekerja dengan aws: SourceVpc ... 72
Bagaimana jalur jaringan yang berbeda tercermin dalam CloudTrail ... 73
Coba Akses Konsol Manajemen AWS Pribadi ... 74
Uji pengaturan dengan Amazon EC2 ... 74
Uji pengaturan dengan Amazon WorkSpaces ... 89
Uji pengaturan VPC dengan kebijakan IAM ... 106
Arsitektur referensi ... 107
AWS Kustomisasi Pengalaman Pengguna ... 109
Memulai ... 110

Prasyarat ..... 110
Mengakses pengaturan UXC di Konsol Manajemen AWS ..... 110
Mengakses pengaturan UXC secara terprogram ..... 111
Pemantauan dengan CloudTrail log ..... 111
Acara manajemen UXC di CloudTrail ..... 112
Contoh acara UXC ..... 31
Keamanan ..... 113
Identity and Access Management ..... 114
AWS kebijakan terkelola ..... 125
AWSManagementConsoleBasicUserAccess ..... 125
AWSManagementConsoleAdministratorAccess ..... 126
Pembaruan kebijakan ..... 127
Penurunan harga di AWS ..... 130
Paragraf, Spasi Baris, dan Garis Horizontal ..... 130
Judul ..... 131
Format Teks ..... 131
Tautan ..... 132
Daftar ..... 132
Tabel dan Tombol (CloudWatch Dasbor) ..... 132
Pemecahan Masalah ..... 134
Halaman tidak dimuat dengan benar ..... 134
Browser saya menampilkan kesalahan 'akses ditolak' saat menghubungkan ke Konsol Manajemen AWS ..... 135
Browser saya menampilkan kesalahan batas waktu saat menghubungkan ke Konsol Manajemen AWS ..... 136
Saya ingin mengubah bahasa Konsol Manajemen AWS tetapi saya tidak dapat menemukan menu pemilihan bahasa di bagian bawah halaman ..... 136
Riwayat dokumen ..... 138
..... cxlii

# Apa itu Konsol Manajemen AWS?

Konsol Manajemen AWSIni adalah aplikasi berbasis web yang berisi dan menyediakan akses terpusat ke semua konsol AWS layanan individu. Anda dapat menggunakan Unified Navigation Konsol Manajemen AWS untuk mencari layanan, melihat notifikasi, mengakses AWS CloudShell, mengakses akun dan informasi penagihan, dan menyesuaikan pengaturan konsol umum Anda. Halaman beranda Konsol Manajemen AWS disebut AWS Console Home. Dari AWS Console Home, Anda dapat mengelola AWS aplikasi Anda dan mengakses semua konsol layanan individual lainnya. Anda juga dapat menyesuaikan AWS Console Home untuk menampilkan informasi bermanfaat lainnya tentang AWS dan sumber daya Anda dengan menggunakan widget. Anda dapat menambahkan, menghapus, dan mengatur ulang widget seperti Baru-baru ini dikunjungi, AWS Kesehatan, dan banyak lagi.

Topik


- Fitur Konsol Manajemen AWS
- Konsol AWS layanan individu di Konsol Manajemen AWS
- Mengakses Konsol Manajemen AWS
- Mengakses Konsol Manajemen AWS dengan perangkat seluler


## Fitur Konsol Manajemen AWS

Fitur penting dari ini Konsol Manajemen AWS meliputi:

- Navigasi ke konsol AWS layanan — Anda dapat menggunakan Navigasi Terpadu untuk mengakses konsol layanan yang baru saja dikunjungi, melihat dan menambahkan layanan ke daftar Favorit, mengakses pengaturan konsol, dan mengakses. Notifikasi Pengguna AWS
- Cari AWS layanan dan AWS informasi lainnya — gunakan Pencarian Terpadu untuk mencari AWS layanan dan fitur, dan AWS memasarkan produk.
- Kustomisasi konsol - Anda dapat menggunakan pengaturan Terpadu untuk menyesuaikan berbagai aspek. Konsol Manajemen AWS Ini termasuk bahasa, Wilayah default, dan banyak lagi.
- Jalankan perintah CLI — dapat AWS CloudShell diakses langsung dari konsol. Anda dapat menggunakan CloudShell untuk menjalankan perintah AWS CLI terhadap layanan favorit Anda.
- Akses semua pemberitahuan AWS acara — Anda dapat menggunakan Konsol Manajemen AWS untuk mengakses notifikasi dari Notifikasi Pengguna AWS dan AWS Health.

- Kustomisasi AWS Console Home - Anda benar-benar dapat menyesuaikan AWS Console Home pengalaman Anda dengan menggunakan widget.
- Buat dan kelola AWS aplikasi — Kelola dan pantau biaya, kesehatan, postur keamanan, dan kinerja aplikasi Anda menggunakan MyApplications di AWS Console Home.
- Mengobrol dengan Amazon Q — Anda bisa mendapatkan jawaban yang didukung asisten kecerdasan buatan (AI) generatif untuk Layanan AWS pertanyaan Anda langsung dari konsol. Anda juga dapat terhubung dengan agen langsung untuk dukungan tambahan.
- Kontrol akses AWS akun di jaringan Anda — Anda dapat menggunakan Akses Konsol Manajemen AWS Pribadi untuk membatasi akses Konsol Manajemen AWS ke kumpulan AWS akun yang diketahui tertentu ketika lalu lintas berasal dari dalam jaringan Anda.

## Konsol AWS layanan individu di Konsol Manajemen AWS

Setiap AWS layanan memiliki konsol layanan tersendiri yang dapat Anda akses di dalam Konsol Manajemen AWS. Pengaturan yang Anda pilih di Pengaturan Terpadu untuk Konsol Manajemen AWS, seperti mode visual dan bahasa default, diterapkan ke semua AWS konsol individual. AWS Konsol layanan menawarkan berbagai alat untuk komputasi awan, serta informasi tentang akun Anda dan tentang penagihan Anda. Jika Anda ingin tahu lebih banyak tentang layanan tertentu dan konsolnya, misalnya Amazon Elastic Compute Cloud, navigasikan ke konsolnya menggunakan Pencarian Terpadu di bilah Konsol Manajemen AWS navigasi dan akses EC2 dokumentasi Amazon dari situs web AWS Dokumentasi.

Saat Anda menavigasi ke konsol AWS layanan individual, Anda masih dapat mengakses fitur Konsol Manajemen AWS menggunakan Navigasi Terpadu di bagian atas konsol. Anda dapat meninggalkan umpan balik untuk konsol layanan individual dengan menavigasi ke konsol tersebut dan memilih Umpan Balik di footer halaman.

## Mengakses Konsol Manajemen AWS

Anda dapat mengakses Konsol Manajemen AWS di https://console.aws.amazon.com/.

## Mengakses Konsol Manajemen AWS dengan perangkat seluler

Konsol Manajemen AWSIni dirancang untuk bekerja pada tablet serta jenis perangkat seluler lainnya:

- Ruang horizontal dan vertikal dimaksimalkan untuk menampilkan lebih banyak konten di layar Anda.

- Tombol dan pemilih berukuran lebih besar agar pengalaman sentuh lebih baik.

Untuk mengakses Konsol Manajemen AWS pada perangkat seluler, Anda harus menggunakan AWS Console Mobile Application. Aplikasi ini tersedia untuk Android dan iOS. Console Mobile Application menyediakan tugas-tugas yang relevan dengan seluler yang merupakan pendamping yang baik untuk pengalaman web lengkap. Misalnya, Anda dapat dengan mudah melihat dan mengelola EC2 instans Amazon dan CloudWatch alarm Amazon yang ada dari ponsel Anda. Untuk informasi lebih lanjut, lihat Apa itu AWS Console Mobile Application? dalam AWS Console Mobile Application User Guide.

Anda dapat mengunduh Console Mobile Application dari Amazon Appstore, Google Play, dan iOS App Store.

# Memulai dengan layanan di Konsol Manajemen AWS

Konsol Manajemen AWS menyediakan beberapa cara untuk menavigasi ke konsol tiap-tiap layanan.

Untuk membuka konsol sebuah layanan

Lakukan salah satu hal berikut ini:

- Di kotak pencarian di bilah navigasi, masukkan semua atau sebagian nama layanan. Di bawah Layanan, pilih layanan yang Anda inginkan dari daftar hasil pencarian. Untuk informasi selengkapnya, lihat Mencari produk, layanan, fitur, dan lainnya menggunakan Unified Search di Konsol Manajemen AWS.
- Di widget Layanan yang baru dikunjungi, pilih nama layanan.
- Di widget Layanan yang baru dikunjungi, pilih Lihat semua AWS layanan. Kemudian, pada halaman Semua AWS layanan, pilih nama layanan.
- Di bilah navigasi, pilih Layanan untuk membuka daftar lengkap layanan. Lalu pilih layanan dari daftar Baru saja dikunjungi atau Semua layanan.

# Menggunakan bilah Konsol Manajemen AWS navigasi melalui Navigasi Terpadu

Topik ini menjelaskan cara menggunakan Navigasi Terpadu. Unified Navigation mengacu pada bilah navigasi yang bertindak sebagai header dan footer konsol. Anda dapat menggunakan Unified Navigation untuk:

- Cari dan akses AWS layanan, fitur, produk, dan lainnya.
- Luncurkan AWS Cloudshell.
- Akses AWS notifikasi dan acara AWS Kesehatan.
- Dapatkan dukungan dari berbagai sumber AWS pengetahuan.
- Konfigurasikan Konsol Manajemen AWS dengan memilih bahasa default, mode visual, Wilayah, dan lainnya.
- Akses akun, organisasi, kuota layanan, dan informasi penagihan.

Topik


- Mengakses menu Layanan di Konsol Manajemen AWS
- Mencari produk, layanan, fitur, dan lainnya menggunakan Unified Search di Konsol Manajemen AWS
- Meluncurkan AWS CloudShell dari bilah navigasi di Konsol Manajemen AWS
- Mengakses AWS notifikasi dan acara Kesehatan
- Mendapatkan Dukungan
- Mengkonfigurasi Konsol Manajemen AWS menggunakan Pengaturan Terpadu
- Mengakses AWS akun, organisasi, kuota layanan, dan informasi penagihan Anda di Konsol Manajemen AWS
- Masuk ke beberapa akun
- AWS Tindakan yang Direkomendasikan di Konsol Manajemen AWS


## Mengakses menu Layanan di Konsol Manajemen AWS

Anda dapat menggunakan menu Layanan, di samping bilah pencarian untuk mengakses layanan yang baru saja Anda kunjungi, melihat daftar Favorit, dan melihat semua AWS layanan. Anda juga

dapat melihat layanan berdasarkan jenis dengan memilih jenis layanan, misalnya Analytics atau Integrasi Aplikasi.

Prosedur berikut menjelaskan cara mengakses menu Layanan.

Untuk mengakses menu Layanan

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih Layanan ().
3. (Opsional) Pilih Baru dikunjungi untuk melihat layanan dan aplikasi yang baru-baru ini berinteraksi dengan Anda.
4. (Opsional) Pilih Favorit untuk melihat daftar Favorit Anda.
5. (Opsional) Pilih Semua aplikasi untuk melihat aplikasi MyApplications Anda.
6. (Opsional) Pilih Semua layanan untuk melihat daftar abjad semua AWS layanan.
7. (Opsional) Pilih jenis layanan untuk melihat AWS layanan berdasarkan jenis.

# Mencari produk, layanan, fitur, dan lainnya menggunakan Unified Search di Konsol Manajemen AWS

Kotak pencarian di bilah navigasi menyediakan alat pencarian terpadu untuk menemukan AWS layanan dan fitur, dokumentasi layanan, AWS Marketplace produk, dan banyak lagi. Cukup masukkan beberapa karakter atau pertanyaan untuk mulai menghasilkan hasil dari semua jenis konten yang tersedia. Setiap kata yang Anda masukkan lebih jauh menyempurnakan hasil Anda. Jenis konten yang tersedia meliputi:

- Layanan
- Fitur
- Dokumen
- Blog
- Artikel Pengetahuan
- Peristiwa
- Tutorial
- Marketplace
- Sumber daya

> **Note**
>
> Anda dapat memfilter hasil pencarian untuk hanya menampilkan sumber daya dengan melakukan pencarian terfokus. Untuk melakukan pencarian terfokus, masukkan `/Resources` di awal kueri Anda di bilah pencarian dan pilih /Resources dari menu tarik-turun. Kemudian masukkan sisa kueri Anda.

Topik


- Mencari AWS produk di Konsol Manajemen AWS
- Menyempurnakan pencarian Anda di Konsol Manajemen AWS
- Melihat fitur layanan di Konsol Manajemen AWS


## Mencari AWS produk di Konsol Manajemen AWS

Prosedur berikut merinci cara mencari AWS produk menggunakan alat pencarian.

Untuk mencari layanan, fitur, dokumentasi, atau AWS Marketplace produk

1. Di kotak pencarian di bilah navigasi Konsol Manajemen AWS, masukkan kueri Anda.
2. Pilih tautan apa pun untuk menavigasi ke tujuan yang Anda inginkan.

> **Tip**
>
> Anda juga dapat menggunakan keyboard untuk menavigasi ke hasil pencarian teratas dengan cepat. Pertama, tekan Alt+s (Windows) atau Option+s (macOS) untuk mengakses bilah pencarian. Kemudian mulai masukkan istilah pencarian Anda. Ketika hasil yang diinginkan muncul di bagian atas daftar, tekan Enter. Sebagai contoh, untuk dengan cepat menavigasi ke konsol Amazon EC2, masukkan ec2 dan tekan Enter.

## Menyempurnakan pencarian Anda di Konsol Manajemen AWS

Anda dapat menyempurnakan pencarian berdasarkan jenis konten dan melihat informasi tambahan tentang hasil penelusuran.

Untuk mempersempit penelusuran Anda ke jenis konten tertentu

1. Di kotak pencarian di bilah navigasi Konsol Manajemen AWS, masukkan kueri Anda.
2. Pilih salah satu jenis konten di samping hasil penelusuran Anda.
3. (Opsional) Untuk melihat semua hasil untuk kategori tertentu:
    - Pilih Tampilkan lebih banyak. Tab baru akan terbuka menampilkan hasilnya.
4. (Opsional) Untuk melihat informasi tambahan tentang hasil pencarian Anda:
    a. Dalam hasil pencarian, arahkan kursor Anda ke hasil pencarian.
    b. Lihat informasi tambahan yang tersedia.

## Melihat fitur layanan di Konsol Manajemen AWS

Anda dapat melihat fitur layanan dari dalam hasil pencarian Anda.

Untuk melihat fitur layanan

1. Di kotak pencarian di bilah navigasi Konsol Manajemen AWS, masukkan kueri Anda.
2. Dalam hasil penelusuran, arahkan kursor Anda ke layanan di Layanan.
3. Pilih salah satu tautan di Fitur teratas.

# Meluncurkan AWS CloudShell dari bilah navigasi di Konsol Manajemen AWS

AWS CloudShell adalah shell berbasis browser dan pra-otentikasi yang dapat Anda luncurkan langsung dari bilah navigasi. Konsol Manajemen AWS Anda dapat menjalankan AWS CLI perintah terhadap layanan menggunakan shell pilihan Anda (Bash, PowerShell, atau Z shell).

Anda dapat meluncurkan CloudShell dari Konsol Manajemen AWS menggunakan salah satu dari dua metode berikut:

- Pilih CloudShell ikon di footer konsol.
- Pilih CloudShell ikon di bilah navigasi konsol.

Untuk informasi selengkapnya tentang layanan ini, lihat Panduan AWS CloudShell Pengguna.

Untuk informasi tentang Wilayah AWS tempat AWS CloudShell tersedia, lihat Daftar Layanan AWS Regional. Pemilihan Wilayah Konsol disinkronkan dengan CloudShell Wilayah. Jika CloudShell tidak tersedia di Wilayah yang dipilih, maka CloudShell akan beroperasi di Wilayah terdekat.

## Mengakses AWS notifikasi dan acara Kesehatan

Anda dapat mengakses beberapa AWS notifikasi dan melihat acara kesehatan dari bilah navigasi. Anda juga dapat mengakses Notifikasi Pengguna AWS untuk melihat semua AWS notifikasi dan AWS Health Dasbor dari bilah navigasi.

Untuk informasi lebih lanjut lihat Apa itu Notifikasi Pengguna AWS? di Panduan Notifikasi Pengguna AWS Pengguna dan Apa itu AWS Health? di Panduan AWS Health Pengguna

Prosedur berikut menjelaskan cara mengakses informasi AWS acara Anda.

Untuk mengakses informasi AWS acara Anda

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon lonceng.
3. Lihat notifikasi dan acara kesehatan Anda.
4. (Opsional) Pilih lihat semua notifikasi untuk menavigasi ke Notifikasi Pengguna konsol.
5. (Opsional) Pilih lihat semua acara Kesehatan untuk menavigasi ke AWS Health konsol.

## Mendapatkan Dukungan

Anda bisa mendapatkan dukungan dengan memilih ikon tanda tanya di bilah navigasi. Dari menu dukungan, Anda dapat memilih untuk:

- Arahkan ke konsol layanan Support Center
- Dapatkan bantuan ahli dari AWS IQ
- Lihat pengetahuan yang dikuratori dari artikel komunitas dan pusat pengetahuan di re:post AWS
- Pergi ke AWS dokumentasi
- Arahkan ke AWS pelatihan
- Arahkan ke Pusat Sumber Daya yang AWS memulai
- Tinggalkan umpan balik untuk konsol layanan apa pun yang sedang Anda akses

> **Note**
>
> Ini juga dapat dilakukan dengan memilih Umpan Balik di footer konsol. Judul modal yang terbuka menunjukkan konsol mana yang saat ini Anda tinggalkan umpan balik

Anda juga bisa mendapatkan bantuan kapan saja di konsol, terhubung dengan agen langsung, dan mengajukan pertanyaan apa pun dengan mengobrol AWS dengan AWS Q. Untuk informasi selengkapnya, lihat ???.

# Mengkonfigurasi Konsol Manajemen AWS menggunakan Pengaturan Terpadu

Topik ini menjelaskan cara mengonfigurasi Anda Konsol Manajemen AWS menggunakan halaman Setelan Terpadu untuk menyetel default yang berlaku untuk semua konsol layanan.

Topik

- Mengkonfigurasi Pengaturan Terpadu di Konsol Manajemen AWS
- Mengkonfigurasi Wilayah dan layanan yang terlihat di Konsol Manajemen AWS
- Memilih Wilayah Anda
- Favorit di Konsol Manajemen AWS
- Mengubah kata sandi Anda di Konsol Manajemen AWS
- Mengubah bahasa Konsol Manajemen AWS

## Mengkonfigurasi Pengaturan Terpadu di Konsol Manajemen AWS

Anda dapat mengonfigurasi pengaturan dan default, seperti tampilan, bahasa, dan Wilayah, dari halaman Pengaturan Konsol Manajemen AWS Terpadu. Anda dapat mengakses Pengaturan Terpadu melalui bilah navigasi di Navigasi Terpadu. Mode visual dan bahasa default juga dapat diatur langsung dari bilah navigasi. Perubahan ini berlaku untuk semua konsol layanan.

> **Important**
>
> Untuk memastikan bahwa pengaturan, layanan favorit, dan layanan yang baru dikunjungi tetap ada secara global, data ini disimpan di semua Wilayah AWS, termasuk Wilayah

yang dinonaktifkan secara default. Wilayah tersebut adalah Afrika (Cape Town), Asia Pasifik (Hong Kong), Asia Pasifik (Hyderabad), Asia Pasifik (Jakarta), Eropa (Milan), Eropa (Spanyol), Eropa (Zurich), Timur Tengah (Bahrain), dan Timur Tengah (UEA). Anda masih perlu mengaktifkan Wilayah secara manual untuk mengaksesnya dan membuat serta mengelola sumber daya di Wilayah tersebut. Jika Anda tidak ingin menyimpan data ini secara keseluruhan Wilayah AWS, pilih Setel ulang semua untuk menghapus pengaturan Anda, lalu pilih untuk tidak mengingat layanan yang baru dikunjungi di manajemen Pengaturan.

Topik


- Mengakses Pengaturan Terpadu di Konsol Manajemen AWS
- Mengatur Ulang Pengaturan Terpadu di Konsol Manajemen AWS
- Mengedit Pengaturan Terpadu di Konsol Manajemen AWS
- Mengubah mode visual dari Konsol Manajemen AWS


## Mengakses Pengaturan Terpadu di Konsol Manajemen AWS

Prosedur berikut menjelaskan cara mengakses Pengaturan Terpadu.

Untuk mengakses Pengaturan Terpadu

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon roda gigi (#).
3. Untuk membuka halaman Pengaturan Terpadu, pilih Lihat semua pengaturan pengguna.

## Mengatur Ulang Pengaturan Terpadu di Konsol Manajemen AWS

Anda dapat menghapus semua konfigurasi Pengaturan Terpadu dan mengembalikan pengaturan default dengan mengatur ulang Pengaturan Terpadu.

> **Note**
>
> Hal ini memengaruhi beberapa area AWS, termasuk layanan favorit dalam navigasi dan menu Layanan, layanan yang baru-baru ini dikunjungi di widget Console Home dan di AWS Console Mobile Application, dan semua pengaturan yang berlaku di seluruh layanan, seperti bahasa default, Wilayah default, dan mode visual.

Untuk mengatur ulang semua Pengaturan Terpadu

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon roda gigi (#).
3. Buka halaman Pengaturan Terpadu dengan memilih Lihat semua pengaturan pengguna.
4. Pilih Atur Ulang semua.

## Mengedit Pengaturan Terpadu di Konsol Manajemen AWS

Prosedur berikut menjelaskan cara mengedit pengaturan pilihan Anda.

Untuk mengedit Setelan Terpadu

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon roda gigi (#).
3. Buka halaman Pengaturan Terpadu dengan memilih Lihat semua pengaturan pengguna.
4. Pilih Edit di samping pengaturan pilihan Anda:

   - Lokalisasi dan Wilayah default:
     - Bahasa memungkinkan Anda memilih bahasa default untuk teks konsol.
     - Wilayah Default memungkinkan Anda memilih Wilayah default yang berlaku setiap kali Anda masuk. Anda dapat memilih salah satu Wilayah yang tersedia untuk akun Anda. Anda juga dapat memilih Wilayah yang terakhir digunakan sebagai default Anda.

       Untuk mempelajari selengkapnya tentang perutean Wilayah di Konsol Manajemen AWS, lihat Memilih Wilayah.
   - Tampilan:
     - Mode visual memungkinkan Anda mengatur konsol ke mode terang, mode gelap, atau mode tampilan default browser Anda.

       Mode gelap adalah fitur beta dan mungkin tidak berlaku di semua konsol AWS layanan.
     - Tampilan bilah favorit mengaktifkan tampilan bilah Favorit antara nama layanan lengkap dengan ikonnya atau hanya ikon layanan.
     - Ukuran ikon bilah favorit mengubah ukuran ikon layanan pada tampilan bilah Favorit antara kecil (16x16 piksel) dan besar (24x24 piksel).
   - Pengaturan manajemen:

- Ingat layanan yang baru dikunjungi memungkinkan Anda memilih apakah Konsol Manajemen AWS mengingat layanan yang baru saja Anda kunjungi. Menonaktifkan ini juga akan menghapus riwayat layanan yang baru saja Anda kunjungi, sehingga Anda tidak akan lagi melihat layanan yang baru saja dikunjungi di menu Layanan AWS Console Mobile Application, atau di widget Console Home.

5. Pilih Simpan perubahan.

### Mengubah mode visual dari Konsol Manajemen AWS

Mode visual Anda menyetel konsol Anda ke mode terang, mode gelap, atau mode tampilan default browser Anda.

Untuk mengubah mode visual dari bilah navigasi

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon roda gigi (#).
3. Untuk mode Visual, pilih Light for light mode, Dark for dark mode, atau Browser default untuk mode tampilan default browser Anda.

## Mengkonfigurasi Wilayah dan layanan yang terlihat di Konsol Manajemen AWS

Administrator akun dapat mengontrol AWS layanan mana Wilayah AWS yang terlihat di Konsol Manajemen AWS navigasi. Pengaturan tingkat akun ini tersedia di tab Pengaturan akun di halaman Pengaturan Terpadu. Saat Anda menyembunyikan Wilayah, itu dihapus dari pemilih Wilayah untuk semua pengguna di akun. Ketika Anda menyembunyikan layanan, itu muncul sebagai tidak tersedia di bagian terpisah dari menu Layanan untuk semua pengguna di akun. Layanan tersembunyi juga berwarna abu-abu di hasil Pencarian Terpadu dan di widget Baru Dikunjungi dan Favorit di Beranda Konsol.

Jika pengguna menavigasi langsung ke Wilayah atau layanan tersembunyi melalui URL, mereka melihat hamparan yang memberi tahu mereka bahwa Wilayah atau layanan disembunyikan di tingkat akun.

> **Note**
>
> Navigasi ke halaman Pengaturan Terpadu selalu tersedia, sehingga administrator tidak dapat mengunci diri dari pengaturan ini. Jika pengguna tidak memiliki izin yang diperlukan, atau jika layanan Kustomisasi Pengalaman AWS Pengguna tidak tersedia, semua Wilayah dan layanan akan terlihat secara default.

Topik


- Prasyarat untuk mengonfigurasi Wilayah dan layanan yang terlihat
- Mengkonfigurasi Wilayah yang terlihat di Konsol Manajemen AWS
- Mengkonfigurasi layanan yang terlihat di Konsol Manajemen AWS


## Prasyarat untuk mengonfigurasi Wilayah dan layanan yang terlihat

Untuk melihat dan mengubah pengaturan Wilayah dan layanan yang terlihat, Anda memerlukan izin IAM tertentu.

- Untuk melihat pengaturan, Anda memerlukan `uxc:GetAccountCustomizations` izin.
- Untuk mengubah pengaturan, Anda memerlukan `uxc:UpdateAccountCustomizations` izin.

Kebijakan AWS terkelola `AWSManagementConsoleBasicUserAccess` dan `AWSManagementConsoleAdministratorAccess` menyertakan izin ini.

Untuk informasi selengkapnya, lihat ???.

## Mengkonfigurasi Wilayah yang terlihat di Konsol Manajemen AWS

Anda dapat memilih mana yang Wilayah AWS muncul di pemilih Wilayah untuk semua pengguna di akun Anda.

Untuk mengonfigurasi Wilayah yang terlihat

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon roda gigi (#).
3. Pilih Lihat semua pengaturan pengguna untuk membuka halaman Pengaturan Terpadu.

4. Pilih tab Pengaturan akun.
5. Untuk Wilayah Terlihat, pilih kotak centang untuk Wilayah yang ingin ditampilkan, atau kosongkan kotak centang untuk Wilayah yang ingin Anda sembunyikan.
6. Pilih Simpan perubahan.

Setelah Anda menyimpan, Wilayah tersembunyi akan dihapus dari pemilih Wilayah untuk semua pengguna di akun.

### Mengkonfigurasi layanan yang terlihat di Konsol Manajemen AWS

Anda dapat memilih AWS layanan mana yang muncul di menu Layanan untuk semua pengguna di akun Anda.

Untuk mengonfigurasi layanan yang terlihat

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon roda gigi (#).
3. Pilih Lihat semua pengaturan pengguna untuk membuka halaman Pengaturan Terpadu.
4. Pilih tab Pengaturan akun.
5. Untuk layanan Terlihat, pilih kotak centang untuk layanan yang ingin ditampilkan, atau kosongkan kotak centang untuk layanan yang ingin Anda sembunyikan.
6. Pilih Simpan perubahan.

Setelah Anda menyimpan, layanan tersembunyi muncul sebagai tidak tersedia di bagian terpisah dari menu Layanan untuk semua pengguna di akun. Layanan tersembunyi juga berwarna abu-abu di hasil Pencarian Terpadu dan di widget Baru Dikunjungi dan Favorit di Beranda Konsol.

## Memilih Wilayah Anda

Untuk banyak layanan, Anda dapat memilih Wilayah AWS yang menentukan di mana sumber daya Anda dikelola. Wilayah adalah kumpulan AWS sumber daya yang terletak di wilayah geografis yang sama. Anda tidak perlu memilih Wilayah untuk Konsol Manajemen AWSatau untuk beberapa layanan, seperti AWS Identity and Access Management. Untuk mempelajari selengkapnya Wilayah AWS, lihat Mengelola Wilayah AWS di Referensi Umum AWS.

> **Note**
>
> Jika Anda telah membuat AWS sumber daya tetapi Anda tidak melihat sumber daya tersebut di konsol, konsol mungkin menampilkan sumber daya dari Wilayah yang berbeda. Beberapa sumber daya (seperti instans Amazon EC2) khusus untuk Wilayah tempat mereka dibuat.

Topik


- Memilih Wilayah dari bilah navigasi di Konsol Manajemen AWS
- Mengatur Wilayah default di Konsol Manajemen AWS


## Memilih Wilayah dari bilah navigasi di Konsol Manajemen AWS

Prosedur berikut merinci bagaimana Anda dapat mengubah Wilayah Anda dari bilah navigasi.

Untuk memilih Wilayah dari bilah navigasi

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih nama Wilayah yang saat ini ditampilkan.
3. Pilih Wilayah untuk beralih ke.

## Mengatur Wilayah default di Konsol Manajemen AWS

Prosedur berikut merinci bagaimana Anda dapat mengubah Wilayah default Anda dari halaman Pengaturan Terpadu.

Untuk mengatur Wilayah default Anda

1. Di bilah navigasi, pilih ikon roda gigi (#).
2. Pilih Lihat semua pengaturan pengguna untuk menavigasi ke halaman Setelan Terpadu.
3. Pilih Edit di samping Lokalisasi dan Wilayah default.
4. Di Wilayah Default, pilih Wilayah.

> **Note**
>
> Jika Anda tidak memilih Wilayah default, Wilayah terakhir yang Anda kunjungi akan menjadi default Anda.

5. Pilih Simpan pengaturan.
6. (Opsional) Pilih Pergi ke Wilayah default baru untuk segera pergi ke Wilayah default baru Anda.

# Favorit di Konsol Manajemen AWS

Untuk mengakses layanan dan aplikasi yang sering digunakan dengan lebih cepat, Anda dapat menyimpan konsol layanan mereka ke daftar Favorit. Anda dapat menambah dan menghapus favorit menggunakan Konsol Manajemen AWS. Saat Anda menambahkan layanan atau aplikasi ke Favorit Anda, itu muncul di bilah cepat Favorit.

Topik

- Menambahkan favorit di Konsol Manajemen AWS
- Mengakses favorit di Konsol Manajemen AWS
- Menghapus favorit di Konsol Manajemen AWS

## Menambahkan favorit di Konsol Manajemen AWS

Anda dapat menambahkan layanan dan aplikasi ke favorit Anda dari menu Layanan dan menu yang baru saja dikunjungi. Anda juga dapat menambahkan layanan ke favorit Anda dengan menggunakan halaman hasil pencarian dari kotak pencarian. Layanan dan aplikasi yang Anda tambahkan ke favorit Anda muncul di bilah cepat Favorit.

Topik

- Quickbar favorit di Konsol Manajemen AWS
- Menambahkan layanan ke favorit Anda di Konsol Manajemen AWS
- Menambahkan aplikasi ke favorit Anda di Konsol Manajemen AWS

## Quickbar favorit di Konsol Manajemen AWS

Quickbar favorit muncul ketika Anda memiliki setidaknya satu AWS layanan atau aplikasi yang ditambahkan ke favorit Anda. Quickbar favorit terletak mengikuti bilah navigasi dan terlihat di semua konsol AWS layanan, sehingga Anda dapat dengan cepat mengakses layanan dan aplikasi favorit Anda. Anda dapat mengatur ulang urutan layanan dan aplikasi di bilah cepat favorit dengan menyeret layanan atau aplikasi ke kiri atau kanan.

## Menambahkan layanan ke favorit Anda di Konsol Manajemen AWS

Anda dapat menambahkan layanan ke favorit Anda dari menu Layanan atau halaman hasil pencarian dari kotak pencarian.

### Services menu

Untuk menambahkan favorit dari menu Layanan

1. Buka Konsol Manajemen AWS.
2. Di bilah navigasi, pilih Layanan ().
3. (Opsional) Tambahkan layanan yang baru saja dikunjungi ke favorit Anda:
   a. Di Baru-baru ini dikunjungi, arahkan kursor Anda ke layanan.
   b. Pilih bintang di sebelah nama layanan.
4. Pilih Semua layanan.
5. Arahkan kursor ke layanan pilihan Anda.
6. Pilih bintang di sebelah nama layanan.

### Search box

Untuk menambahkan favorit dari kotak pencarian

1. Buka Konsol Manajemen AWS.
2. Masukkan nama layanan di kotak pencarian.
3. Di halaman hasil pencarian, pilih bintang di sebelah nama layanan.

> **Note**
>
> Setelah Anda menambahkan layanan ke favorit Anda, itu ditambahkan ke bilah cepat favorit mengikuti bilah navigasi.

Menambahkan aplikasi ke favorit Anda di Konsol Manajemen AWS

Anda dapat menambahkan aplikasi ke favorit Anda dari menu Layanan.

Untuk menambahkan favorit dari menu Layanan

1. Buka Konsol Manajemen AWS.
2. Di bilah navigasi, pilih Layanan ().
3. (Opsional) Tambahkan aplikasi yang baru saja dikunjungi ke favorit Anda:
   a. Di Baru-baru ini dikunjungi, arahkan kursor Anda ke aplikasi.
   b. Pilih bintang di sebelah nama aplikasi.
4. Pilih Aplikasi.
5. Arahkan kursor Anda ke aplikasi yang Anda pilih.
6. Pilih bintang di sebelah nama aplikasi.

> **Note**
>
> Setelah Anda menambahkan aplikasi ke favorit Anda, itu ditambahkan ke bilah cepat favorit mengikuti bilah navigasi.

## Mengakses favorit di Konsol Manajemen AWS

Anda dapat mengakses layanan dan aplikasi yang ditambahkan ke favorit Anda dari menu Layanan, bilah cepat favorit, dan widget Favorit.

Services menu

Untuk mengakses favorit Anda dari menu Layanan

1. Buka Konsol Manajemen AWS.

2. Di bilah navigasi, pilih Layanan ().
3. Pilih Favorit.
4. Lihat layanan dan aplikasi yang Anda tambahkan ke favorit Anda.
5. (Opsional) Lihat sumber daya aplikasi:
    a. Pilih aplikasi.
    b. (Opsional) Pilih tampilan.
    c. Lihat sumber daya Anda.
    d. (Opsional) Pilih filter. Anda dapat memfilter sumber daya Anda berdasarkan Properti atau Tag. Untuk informasi selengkapnya, lihat Referensi sintaks kueri penelusuran untuk Resource Explorer di Panduan Penjelajah Sumber Daya AWS Pengguna.
    e. (Opsional) Pilih sumber daya untuk melihatnya di konsol layanan yang relevan.

> **Tip**
>
> Anda dapat melanjutkan penelusuran sumber daya yang Anda tinggalkan dengan memilih Layanan (). Filter pencarian yang Anda terapkan juga akan bertahan.

Favorites quickbar

Untuk mengakses favorit Anda dari bilah cepat favorit

1. Buka Konsol Manajemen AWS.
2. Lihat layanan dan aplikasi di bilah cepat favorit.

Favorites widget

Untuk mengakses favorit Anda dari widget Favorit

1. Buka Konsol Manajemen AWS.
2. (Opsional) Tambahkan widget Favorit jika Anda tidak memilikinya:
    a. Pilih tombol+Tambahkan widget di halaman Beranda Konsol.

b. Di menu Tambahkan widget, seret widget Favorit dengan menggunakan ikon dan letakkan di halaman Beranda Konsol Anda.

3. Lihat layanan dan aplikasi di widget Favorit.

Untuk informasi selengkapnya tentang widget, lihatthe section called “Bekerja dengan Widget”.

## Menghapus favorit di Konsol Manajemen AWS

Anda dapat menghapus layanan dan aplikasi dari favorit Anda menggunakan menu Layanan. Anda juga dapat menghapus layanan dengan menggunakan halaman hasil pencarian dari bilah pencarian.

Services menu

Untuk menghapus favorit dari menu Layanan

1. Buka Konsol Manajemen AWS.
2. Di bilah navigasi, pilih Layanan.
3. Pilih Favorit.
4. Batalkan pilihan bintang di sebelah layanan atau aplikasi.

Search box

> **Note**
>
> Saat ini, Anda hanya dapat menghapus layanan menggunakan halaman hasil pencarian dari bilah pencarian.

Untuk menghapus favorit dari kotak pencarian

1. Buka Konsol Manajemen AWS.
2. Masukkan nama layanan di kotak pencarian.
3. Di halaman hasil pencarian, batalkan pilihan bintang di sebelah nama layanan.

# Mengubah kata sandi Anda di Konsol Manajemen AWS

Anda mungkin dapat mengubah kata sandi Anda dari Konsol Manajemen AWStergantung pada jenis pengguna dan izin Anda. Topik berikut menjelaskan cara mengubah kata sandi Anda untuk setiap jenis pengguna.

Topik


- Pengguna root di Konsol Manajemen AWS
- Pengguna IAM di Konsol Manajemen AWS
- Pengguna Pusat Identitas IAM di Konsol Manajemen AWS
- Identitas federasi di Konsol Manajemen AWS


## Pengguna root di Konsol Manajemen AWS

Pengguna root dapat mengubah kata sandi mereka langsung dari file Konsol Manajemen AWS. Pengguna Root adalah pemilik akun dengan akses lengkap ke semua AWS layanan dan sumber daya. Anda adalah pengguna root jika Anda membuat AWS akun dan Anda masuk menggunakan email pengguna root dan kata sandi Anda. Untuk informasi selengkapnya, lihat Pengguna root di Panduan AWS IAM Identity Center Pengguna.

Untuk mengubah kata sandi Anda sebagai pengguna Root

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih nama akun Anda.
3. Pilih Kredensial keamanan.
4. Opsi yang ditampilkan akan bervariasi tergantung pada Akun AWS jenis Anda. Ikuti petunjuk yang ditampilkan di konsol untuk mengubah kata sandi Anda.
5. Masukkan kata sandi saat ini sekali dan kata sandi baru dua kali.

   Kata sandi baru harus memiliki panjang minimal delapan karakter dan harus menyertakan yang berikut:

   - Setidaknya satu simbol
   - Setidaknya satu nomor
   - Setidaknya satu huruf besar
   - Setidaknya satu huruf kecil

6. Pilih Ubah Kata Sandi atau Simpan perubahan.

## Pengguna IAM di Konsol Manajemen AWS

Pengguna IAM mungkin dapat mengubah kata sandi mereka dari Konsol Manajemen AWS tergantung pada izin mereka. Jika tidak, mereka harus menggunakan portal AWS akses. Pengguna IAM adalah identitas dalam AWS akun Anda yang diberikan izin khusus khusus. Anda adalah pengguna IAM jika Anda tidak membuat AWS akun dan administrator atau karyawan help desk memberikan kredensi masuk Anda yang menyertakan ID AWS akun atau alias akun, nama pengguna IAM, dan kata sandi. Untuk informasi selengkapnya, lihat pengguna IAM di Panduan AWS Sign-In Pengguna.

Jika Anda memiliki izin dari kebijakan berikut: AWS: Memungkinkan pengguna IAM mengubah kata sandi konsol mereka sendiri di halaman Kredensial keamanan, Anda dapat mengubah kata sandi dari konsol. Untuk informasi selengkapnya, lihat Cara pengguna IAM mengubah kata sandi mereka sendiri di Panduan AWS Identity and Access Management Pengguna.

Jika Anda tidak memiliki izin yang diperlukan untuk mengubah kata sandi Anda dari Konsol Manajemen AWS lihat, Mengatur ulang kata sandi AWS IAM Identity Center pengguna Anda di Panduan Pengguna.AWS IAM Identity Center

## Pengguna Pusat Identitas IAM di Konsol Manajemen AWS

AWS IAM Identity Center pengguna harus mengubah kata sandi mereka dari portal AWS akses. Untuk informasi selengkapnya, lihat Menyetel ulang kata sandi AWS IAM Identity Center pengguna di Panduan AWS IAM Identity Center Pengguna.

Pengguna IAM Identity Center adalah pengguna yang AWS akunnya merupakan bagian dari AWS Organizations siapa yang masuk melalui portal AWS akses dengan URL unik. Pengguna ini dapat dibuat langsung di pengguna di Pusat Identitas IAM atau di direktori Aktif atau penyedia identitas eksternal lainnya. Untuk informasi selengkapnya, lihat AWS IAM Identity Center pengguna di Panduan AWS Sign-In Pengguna.

## Identitas federasi di Konsol Manajemen AWS

Pengguna identitas federasi harus mengubah kata sandi mereka dari portal AWS akses. Untuk informasi selengkapnya, lihat Menyetel ulang kata sandi AWS IAM Identity Center pengguna di Panduan AWS IAM Identity Center Pengguna.

Pengguna identitas gabungan masuk menggunakan penyedia identitas eksternal (iDP). Anda adalah identitas federasi jika Anda:

- Akses AWS akun atau sumber daya Anda dengan kredensi pihak ketiga seperti Login with Amazon, Facebook, atau Google.
- Gunakan kredensi yang sama untuk masuk ke sistem dan AWS layanan perusahaan dan Anda menggunakan portal perusahaan khusus untuk masuk. AWS

Untuk informasi selengkapnya, lihat Identitas gabungan di Panduan AWS Sign-In Pengguna. .

## Mengubah bahasa Konsol Manajemen AWS

AWS Console Home Pengalaman termasuk halaman Pengaturan Terpadu di mana Anda dapat mengubah bahasa default untuk AWS layanan di Konsol Manajemen AWS. Anda juga dapat mengubah bahasa default dengan cepat dari menu pengaturan dari bilah navigasi.

> **Note**
>
> Prosedur berikut mengubah bahasa untuk semua konsol AWS layanan, tetapi tidak untuk AWS dokumentasi. Untuk mengubah bahasa yang digunakan untuk dokumentasi, gunakan menu bahasa di kanan atas halaman dokumentasi apa pun.

Topik

- Bahasa yang didukung
- Mengubah bahasa default dari bilah navigasi di Konsol Manajemen AWS
- Mengubah bahasa default melalui Pengaturan Terpadu di Konsol Manajemen AWS

### Bahasa yang didukung

Konsol Manajemen AWS Saat ini mendukung bahasa-bahasa berikut:

- Inggris (US)
- Inggris (UK)
- Bahasa Indonesia
- Bahasa Jerman

- Bahasa Spanyol
- Prancis
- Bahasa Jepang
- Bahasa Italia
- Bahasa Portugis
- Bahasa Korea
- Mandarin (Sederhana)
- Mandarin (Tradisional)
- Turki

## Mengubah bahasa default dari bilah navigasi di Konsol Manajemen AWS

Prosedur berikut merinci cara mengubah bahasa default Anda langsung dari bilah navigasi.

Untuk mengubah bahasa default dari bilah navigasi

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon roda gigi (#).
3. Untuk Bahasa, pilih salah satu Browser default atau bahasa pilihan dari daftar dropdown.

## Mengubah bahasa default melalui Pengaturan Terpadu di Konsol Manajemen AWS

Prosedur berikut merinci cara mengubah bahasa default Anda dari halaman Pengaturan Terpadu.

Untuk mengubah bahasa default di Pengaturan Terpadu

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih ikon roda gigi (#).
3. Untuk membuka halaman Pengaturan Terpadu, pilih Lihat semua pengaturan pengguna.
4. Di Pengaturan Terpadu, pilih Edit di samping Lokalisasi dan Wilayah default.
5. Untuk memilih bahasa yang Anda inginkan untuk konsol, pilih salah satu opsi berikut:

    - Pilih default Browser dari daftar dropdown, lalu pilih Simpan pengaturan.

      Teks konsol untuk semua AWS layanan muncul dalam bahasa pilihan Anda yang telah Anda tetapkan di pengaturan browser Anda.

> **Note**
>
> Browser default hanya mendukung bahasa yang didukung oleh Konsol Manajemen AWS.

- Pilih bahasa pilihan dari daftar dropdown, lalu pilih Simpan pengaturan.

  Teks konsol untuk semua AWS layanan muncul dalam bahasa pilihan Anda.

## Mengakses AWS akun, organisasi, kuota layanan, dan informasi penagihan Anda di Konsol Manajemen AWS

Jika Anda memiliki izin yang diperlukan, Anda dapat mengakses informasi tentang AWS akun Anda, kuota layanan, organisasi, dan informasi penagihan dari konsol.

> **Note**
>
> Konsol Manajemen AWS Hanya menyediakan akses ke akun, organisasi, kuota layanan, dan informasi penagihan. Layanan ini memiliki konsol terpisah mereka sendiri. Untuk informasi selengkapnya, lihat berikut ini:
>
> - Kelola AWS akun Anda di Panduan AWS Account Management Referensi.
> - Apa itu AWS Organizations? dalam AWS Organizations User Guide.
> - Apa itu Service Quotas? dalam Panduan Pengguna Service Quotas.
> - Menggunakan AWS Manajemen Penagihan dan Biaya halaman beranda di Panduan Pengguna AWS Penagihan.

> **Tip**
>
> Anda juga bisa mendapatkan informasi selengkapnya tentang topik ini dengan menanyakan Amazon Q. Untuk informasi selengkapnya, lihat Mengobrol dengan Pengembang Amazon Q.

Topik

- Mengakses informasi akun di Konsol Manajemen AWS

- Mengakses informasi organisasi di Konsol Manajemen AWS
- Mengakses informasi kuota layanan di Konsol Manajemen AWS
- Mengakses informasi penagihan di Konsol Manajemen AWS

## Mengakses informasi akun di Konsol Manajemen AWS

Jika Anda memiliki izin yang diperlukan, Anda dapat mengakses informasi tentang AWS akun Anda dari konsol.

Untuk mengakses informasi akun Anda

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih nama akun Anda.
3. Pilih Akun.
4. Lihat informasi akun Anda.

> **Note**
>
> Jika Anda ingin menutup AWS akun, lihat Menutup AWS akun di Panduan AWS Account Management Referensi.

## Mengakses informasi organisasi di Konsol Manajemen AWS

Jika Anda memiliki izin yang diperlukan, Anda dapat mengakses informasi tentang AWS organisasi Anda dari konsol.

Untuk mengakses informasi organisasi

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih nama akun Anda.
3. Pilih Organizations.
4. Lihat informasi organisasi Anda.

## Mengakses informasi kuota layanan di Konsol Manajemen AWS

Jika Anda memiliki izin yang diperlukan, Anda dapat mengakses informasi tentang kuota layanan dari konsol.

Untuk mengakses informasi kuota layanan

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih nama akun Anda.
3. Pilih Service Quotas.
4. Lihat dan kelola informasi kuota layanan Anda.

## Mengakses informasi penagihan di Konsol Manajemen AWS

Jika Anda memiliki izin yang diperlukan, Anda dapat mengakses informasi tentang AWS tagihan Anda dari konsol.

Untuk mengakses informasi penagihan Anda

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih nama akun Anda.
3. Pilih Billing and Cost Management.
4. Gunakan AWS Manajemen Penagihan dan Biaya dasbor untuk menemukan ringkasan dan rincian pengeluaran bulanan Anda.

# Masuk ke beberapa akun

Anda dapat masuk hingga lima identitas berbeda secara bersamaan dalam satu browser web di Konsol Manajemen AWS. Ini bisa berupa kombinasi root, IAM, atau peran federasi di akun yang berbeda atau di akun yang sama. Setiap identitas yang Anda masuk untuk membuka instancenya sendiri Konsol Manajemen AWS di tab baru.

Saat Anda mengaktifkan dukungan multi-sesi, URL konsol berisi subdomain (misalnya,`https://000000000000-aaaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1`). Pastikan untuk memperbarui bookmark dan tautan konsol Anda.

> **Note**
>
> Anda harus ikut serta dalam dukungan multi-sesi dengan memilih Aktifkan multi-sesi di menu akun di Konsol Manajemen AWS, atau dengan memilih Aktifkan multi-sesi di/. https://console.aws.amazon.com Anda dapat memilih keluar dari multi-sesi kapan saja dengan memilih Nonaktifkan multi-sesi di https://console.aws.amazon.com/atau dengan membersihkan cookie browser Anda. Keikutsertaan adalah khusus browser.

Untuk masuk ke beberapa identitas

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih nama akun Anda.
3. Pilih Tambah sesi dan pilih Masuk. Tab baru akan terbuka bagi Anda untuk masuk.

   > **Note**
   >
   > Untuk informasi selengkapnya tentang masuk sebagai root atau pengguna IAM, lihat Konsol Manajemen AWS Masuk ke Panduan Pengguna AWS Masuk.

4. Masukkan kredensi Anda.
5. Pilih Masuk. Konsol Manajemen AWS Beban di tab ini sebagai AWS identitas yang Anda pilih.
6. (Opsional) Untuk bergabung menjadi peran tambahan

   a. Di portal AWS IAM Identity Center akses atau portal single-sign on (SSO) Anda, masuk ke peran tambahan.

   b. Di Konsol Manajemen AWS pilih nama akun Anda.

   c. Lihat sesi tambahan yang dapat Anda pilih.

# AWS Tindakan yang Direkomendasikan di Konsol Manajemen AWS

AWS Tindakan yang Direkomendasikan membantu Anda bekerja lebih efisien Konsol Manajemen AWS dengan memberikan saran kontekstual untuk menyelesaikan tugas dan menerapkan praktik terbaik. Ketika rekomendasi yang relevan tersedia, tombol dinamis muncul yang dapat Anda gunakan untuk mengambil tindakan cepat berdasarkan saran ini.

> **Note**
>
> AWS Tindakan yang Direkomendasikan menganalisis status sumber daya untuk memberikan saran tetapi tidak memproses data pengguna.

Topik


- Fitur Tindakan yang AWS Direkomendasikan
- Menggunakan tindakan yang disarankan
- Mencatat panggilan API Tindakan yang AWS Direkomendasikan menggunakan AWS CloudTrail


## Fitur Tindakan yang AWS Direkomendasikan

- Rekomendasi tindakan — Dapatkan saran yang relevan berdasarkan status sumber daya, praktik terbaik, dan pola penggunaan umum
- Tindakan sekali klik - Selesaikan tindakan yang disarankan langsung dari pesan sukses atau tampilan sumber daya
- Panel sisi kanan terintegrasi - Akses panel samping terintegrasi untuk menerapkan saran tanpa mengganggu alur kerja Anda
- Dukungan multi-layanan - Dapatkan rekomendasi di berbagai AWS layanan

## Menggunakan tindakan yang disarankan

Untuk menggunakan tindakan yang disarankan

1. Masuk ke Konsol Manajemen AWS
2. Cari tombol # Tindakan yang disarankan.

   > **Note**
   >
   > Tombol tindakan yang disarankan dapat muncul di mana saja di Konsol Manajemen AWS dan hanya dapat diakses ketika tindakan yang disarankan tersedia.

3. Pilih tombol untuk melihat tindakan yang tersedia.
4. Jalankan rekomendasi secara langsung atau melalui panel samping.

# Mencatat panggilan API Tindakan yang AWS Direkomendasikan menggunakan AWS CloudTrail

AWS Tindakan yang Direkomendasikan terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. CloudTrail menangkap semua panggilan API untuk Tindakan yang AWS Direkomendasikan sebagai peristiwa. Panggilan yang diambil mencakup panggilan dari panggilan Konsol Manajemen AWS dan kode ke operasi API Tindakan yang AWS Direkomendasikan. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Tindakan yang AWS Disarankan, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

## AWS Acara manajemen Tindakan yang Direkomendasikan di CloudTrail

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. Ini juga dikenal sebagai operasi bidang kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

AWS Tindakan yang AWS Direkomendasikan mencatat semua tindakan yang direkomendasikan mengontrol operasi pesawat sebagai peristiwa manajemen.

## AWS Contoh acara Tindakan yang Direkomendasikan

Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang operasi API yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan CloudTrail peristiwa yang menunjukkan operasi.

```
{
```

```
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  },
  "responseElements": null,
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "EXAMPLE",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
    "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
    "accountId": "12345678909",
    "accessKeyId": "ASIARZDBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AROARZDBHEXAMPLE",
          "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
          "accountId": "12345678909",
          "userName": "EXAMPLE"
        },
        "attributes": {
          "creationDate": "2025-09-03T03:52:00Z",
          "mfaAuthenticated": "false"
        }
      },
    "invokedBy": "action-recommendations.amazonaws.com"
  }
}
```

Untuk informasi tentang konten CloudTrail rekaman, lihat konten CloudTrail rekaman di Panduan AWS CloudTrail Pengguna.

# Menggunakan AWS Console Home di Konsol Manajemen AWS

Topik ini menjelaskan cara menggunakan AWS Console Home, termasuk cara menyesuaikan halaman Beranda Konsol Anda. Console Home adalah halaman beranda dari Konsol Manajemen AWS. Saat pertama kali masuk ke konsol, Anda mendarat di halaman Beranda Konsol. Anda dapat menyesuaikan halaman Beranda Konsol menggunakan widget dan aplikasi. Widget memungkinkan Anda menambahkan komponen khusus yang melacak informasi tentang AWS layanan dan sumber daya Anda. Aplikasi memungkinkan Anda untuk mengelompokkan AWS sumber daya dan metadata Anda. Anda dapat mengelola aplikasi menggunakan MyApplications. Anda juga dapat menggunakan Console Home untuk melihat daftar semua AWS layanan dan mengobrol dengan Amazon Q.

Topik


- Melihat semua AWS layanan di AWS Console Home
- Bekerja dengan widget di AWS Console Home
- Apa itu MyApplications? AWS Console Home
- Mengobrol dengan Pengembang Amazon Q di AWS Console Home


## Melihat semua AWS layanan di AWS Console Home

Anda dapat melihat daftar semua AWS layanan dan mengakses konsol mereka dari Console Home.

Untuk mengakses daftar lengkap AWS layanan

1. Masuk ke Konsol Manajemen AWS.
2. Perluas menu Beranda Konsol dengan memilih ikon hamburger (☰).
3. Pilih Semua layanan.
4. Pilih AWS layanan untuk menavigasi ke konsolnya.

## Bekerja dengan widget di AWS Console Home

Dasbor Beranda Konsol menyertakan widget yang menampilkan informasi penting tentang AWS lingkungan Anda dan menyediakan pintasan ke layanan Anda. Anda dapat menyesuaikan

pengalaman Anda dengan menambahkan dan menghapus widget, mengatur ulang, atau mengubah ukurannya.

## Mengelola widget

Anda dapat mengelola widget dengan menambahkan, menghapus, mengatur ulang, dan mengubah ukurannya. Widget default dapat saya hapus dan ditambahkan lagi. Anda juga dapat mengatur ulang Beranda Konsol ke tata letak default dan meminta widget baru.

Untuk menambahkan widget

1. Di kanan atas atau bawah dasbor Console Home, pilih tombol+Tambah widget.
2. Pilih indikator seret, diwakili oleh enam titik vertikal () di kiri atas bilah judul widget, lalu seret ke dasbor Beranda Konsol Anda.

Untuk menghapus widget

1. Pilih elipsis, diwakili oleh tiga titik vertikal () di kanan atas bilah judul widget.
2. Pilih Hapus widget.

Untuk mengatur ulang widget Anda

- Pilih indikator seret, diwakili oleh enam titik vertikal () di kiri atas bilah judul widget, lalu seret widget ke lokasi baru di dasbor Beranda Konsol Anda.

Untuk mengubah ukuran widget

- Pilih ikon mengubah ukuran di kanan bawah widget, lalu seret untuk mengubah ukuran widget.

Jika Anda ingin memulai dari awal dengan mengatur dan mengatur widget Anda, Anda dapat mengatur ulang dasbor Beranda Konsol ke tata letak default. Ini akan mengembalikan perubahan Anda ke tata letak dasbor Beranda Konsol, dan mengembalikan semua widget ke lokasi dan ukuran defaultnya.

Untuk mengatur ulang halaman ke tata letak default

1. Di kanan atas halaman, pilih tombol Reset to default layout.

2. Untuk mengonfirmasi, pilih Reset.

> **Note**
>
> Ini akan mengembalikan semua perubahan Anda ke tata letak dasbor Beranda Konsol.

Untuk meminta widget baru di dasbor Beranda Konsol

1. Di kiri bawah dasbor Console Home, pilih Ingin melihat widget lain? Beritahu kami!

   Jelaskan widget yang ingin Anda lihat ditambahkan di dasbor Beranda Konsol.
2. Pilih Kirim.

> **Note**
>
> Saran Anda ditinjau secara berkala dan widget baru dapat ditambahkan di pembaruan masa depan ke file. Konsol Manajemen AWS

# Apa itu MyApplications? AWS Console Home

MyApplications adalah perpanjangan dari Console Home yang membantu Anda mengelola dan memantau biaya, kesehatan, postur keamanan, dan kinerja aplikasi Anda. AWS Aplikasi memungkinkan Anda mengelompokkan sumber daya dan metadata. Anda dapat mengakses semua aplikasi di akun Anda, metrik utama di semua aplikasi, dan ikhtisar metrik biaya, keamanan, dan operasi serta wawasan dari beberapa konsol layanan dari satu tampilan di Konsol Manajemen AWS. myApplications mencakup hal-hal berikut:

- Widget aplikasi di halaman Beranda Konsol
- MyApplications yang dapat Anda gunakan untuk melihat biaya sumber daya aplikasi dan temuan keamanan
- Dasbor MyApplications yang menyediakan tampilan metrik aplikasi utama seperti biaya, kinerja, dan temuan keamanan

Topik

- Fitur MyApplications
- Layanan terkait
- Mengakses MyApplications
- Harga
- Wilayah yang Didukung untuk MyApplications
- Aplikasi di MyApplications
- Sumber daya di MyApplications
- Dasbor MyApplications di AWS Console Home


## Fitur MyApplications

- Buat aplikasi — Buat aplikasi baru dan atur sumber dayanya. Aplikasi Anda secara otomatis ditampilkan di MyApplications, sehingga Anda dapat mengambil tindakan di Konsol Manajemen AWS,, CLI APIs, dan. SDKs Infrastruktur sebagai kode (IAc) dihasilkan saat Anda membuat aplikasi dan dapat diakses dari dasbor MyApplication. IAc dapat digunakan dalam alat IAc termasuk AWS CloudFormation dan Terraform.
- Akses aplikasi Anda — Anda dapat dengan cepat mengakses salah satu aplikasi Anda dari widget MyApplications dengan memilihnya.
- Mengakses sumber daya Anda — Anda dapat dengan cepat melihat sumber daya aplikasi Anda dari menu Layanan dengan memilih aplikasi. Ketika Anda memilih sumber daya, Anda langsung menuju ke konsol layanan yang relevan. Tempat Anda di tabel sumber daya disimpan, sehingga Anda dapat melanjutkan penelusuran kapan saja dari menu Layanan.
- Bandingkan metrik aplikasi — Gunakan MyApplications untuk membandingkan metrik utama untuk aplikasi seperti biaya sumber daya aplikasi dan jumlah temuan keamanan penting untuk beberapa aplikasi.
- Memantau dan mengelola aplikasi - Menilai kesehatan dan kinerja aplikasi menggunakan alarm, kenari, dan tujuan tingkat layanan dari Amazon CloudWatch, temuan dari AWS Security Hub CSPM, dan tren biaya dari. AWS Cost Explorer Service Anda juga dapat menemukan ringkasan dan pengoptimalan metrik komputasi serta mengelola kepatuhan sumber daya dan status konfigurasi dari. AWS Systems Manager

## Layanan terkait

MyApplications menggunakan layanan berikut:

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- Penjelajah Sumber Daya AWS
- AWS Security Hub CSPM
- Systems Manager
- AWS Service Catalog
- Penandaan

## Mengakses MyApplications

Anda dapat mengakses MyApplications dari Konsol Manajemen AWSdengan memilih MyApplications di sidebar kiri.

## Harga

MyApplications on AWS ditawarkan tanpa biaya tambahan. Tidak ada biaya set-up atau komitmen di muka. Biaya penggunaan untuk sumber daya dan layanan dasar yang diringkas dasbor MyApplication masih berlaku pada tarif yang dipublikasikan untuk sumber daya tersebut.

## Wilayah yang Didukung untuk MyApplications

MyApplications tersedia sebagai berikut: Wilayah AWS

- AS Timur (Ohio)
- AS Timur (Virginia Utara)
- AS Barat (California Utara)
- AS Barat (Oregon)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Osaka)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)

- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- Kanada (Pusat)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Paris)
- Eropa (Stockholm)
- Amerika Selatan (Sao Paulo)

### Wilayah Keikutsertaan

Wilayah Keikutsertaan tidak diaktifkan secara default. Anda harus mengaktifkan Wilayah ini secara manual untuk menggunakannya dengan MyApplications. Untuk informasi selengkapnya Wilayah AWS, lihat Mengelola Wilayah AWS. Wilayah keikutsertaan berikut didukung:

- Africa (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Melbourne)
- Eropa (Milan)
- Eropa (Spanyol)
- Eropa (Zürich)
- Timur Tengah (Bahrain)
- Middle East (UAE)
- Israel (Tel Aviv)

## Aplikasi di MyApplications

Aplikasi memungkinkan Anda untuk mengelompokkan sumber daya dan metadata Anda. Anda dapat mengelola aplikasi Anda dengan membuat, melakukan orientasi, melihat, mengedit, atau

menghapusnya. Anda juga dapat membuat cuplikan kode untuk secara otomatis menambahkan sumber daya baru ke aplikasi.

> **Note**
>
> Anda juga dapat menambahkan aplikasi ke Favorit Anda sehingga lebih mudah diakses. Untuk informasi selengkapnya, lihat ???.

Topik

- Membuat aplikasi di MyApplications
- Onboard AppRegistry Aplikasi yang ada di MyApplications
- Melihat aplikasi di MyApplications
- Mengedit aplikasi di MyApplications
- Menghapus aplikasi di MyApplications
- Membuat cuplikan kode di MyApplications

## Membuat aplikasi di MyApplications

Anda dapat membuat aplikasi baru atau the section called “Aplikasi orientasi” dibuat sebelum 8 November 2023 untuk memulai dengan MyApplications. Saat Anda membuat aplikasi baru, Anda dapat menambahkan sumber daya dengan mencarinya dan memilihnya atau dengan menggunakan tag yang ada.

Untuk membuat aplikasi baru

1. Masuk ke Konsol Manajemen AWS.
2. Perluas sidebar kiri dan pilih MyApplications.
3. Pilih Create application (Buat aplikasi).
4. Masukkan nama aplikasi.
5. (Opsional) Masukkan deskripsi aplikasi.
6. (Opsional) Tambahkan tag. Tag adalah pasangan nilai kunci yang diterapkan ke sumber daya untuk menyimpan metadata tentang sumber daya tersebut.

> **Note**
>
> Tag AWS aplikasi secara otomatis diterapkan ke aplikasi yang baru dibuat. Untuk informasi selengkapnya, lihat Tag AWS aplikasi di Panduan AWS Service Catalog AppRegistry Administrator.

7. (Opsional) Tambahkan grup atribut. Anda dapat menggunakan grup atribut untuk menyimpan metadata aplikasi.
8. Pilih Berikutnya.
9. (Opsional) Tambahkan sumber daya:

   Search and select resources

   > **Note**
   >
   > Untuk mencari dan menambahkan sumber daya, Anda harus mengaktifkan Penjelajah Sumber Daya AWS. Untuk informasi selengkapnya, lihat Memulai dengan Penjelajah Sumber Daya AWS.
   > Semua sumber daya yang ditambahkan ditandai dengan tag AWS aplikasi.

   Untuk menambahkan sumber daya menggunakan pencarian

   1. Pilih Cari dan pilih sumber daya.
   2. Pilih Pilih sumber daya.
   3. (Opsional) Pilih tampilan.
   4. Cari sumber daya Anda. Anda dapat mencari berdasarkan kata kunci, nama atau jenis, atau memilih jenis sumber daya.

      > **Note**
      >
      > Jika Anda tidak dapat menemukan sumber daya yang Anda cari, pecahkan masalah dengan. Penjelajah Sumber Daya AWS Untuk informasi selengkapnya, lihat Memecahkan masalah penelusuran Resource Explorer di Panduan Pengguna Resource Explorer.

5. Pilih kotak centang di sebelah sumber daya yang ingin Anda tambahkan.
6. Pilih Tambahkan.
7. Pilih Berikutnya.
8. Tinjau pilihan Anda.

Automatically add resources using tags

Saat membuat aplikasi, Anda dapat mengumpulkan sumber daya secara massal dengan menentukan pasangan nilai kunci tag yang ada. Dengan metode ini, AWS secara otomatis menerapkan `awsApplication` tag ke semua sumber daya yang ditandai dengan pasangan nilai kunci yang ditentukan, dan membuat sinkronisasi tag untuk sumber daya aplikasi secara default. Dengan sinkronisasi tag diaktifkan, sumber daya apa pun yang ditandai dengan pasangan nilai kunci tag yang ditentukan secara otomatis ditambahkan ke aplikasi. Untuk informasi tentang menyelesaikan kesalahan sinkronisasi tag, lihat. the section called “Menyelesaikan kesalahan sinkronisasi tag di MyApplications”

> **Note**
>
> Menambahkan sumber daya ke aplikasi menggunakan tag memerlukan izin untuk membuat AppRegistry aplikasi, mengelompokkan dan sumber daya ungroup, serta menandai dan menghapus tag sumber daya. Anda dapat menambahkan kebijakan `ResourceGroupsTaggingAPITagUntagSupportedResources` AWS terkelola Resource Groups, atau Anda dapat membuat dan memelihara kebijakan kustom Anda sendiri. Izin berikut harus ditambahkan ke pernyataan kebijakan pengguna di IAM:
>
> - `servicecatalog:CreateApplication`
> - `resource-groups:GroupResources`
> - `resource-groups:UngroupResources`
> - `tag:TagResources`
> - `tag:UntagResources`

Untuk menambahkan sumber daya menggunakan tag yang ada

1. Pilih Tambahkan sumber daya secara otomatis menggunakan tag.
2. Pilih kunci dan nilai tag yang ada:

   a. Pilih Peran yang digunakan untuk menandai sumber daya. Untuk informasi selengkapnya, lihat Izin yang diperlukan sinkronisasi Tag di Panduan Administrator AWS Service Catalog AppRegistry .

   b. Pilih tombol Tag.

   c. Pilih nilai Tag.

   d. (Opsional) Pilih Pratinjau sumber daya untuk melihat pratinjau sumber daya mana yang ditandai dengan pasangan nilai kunci tag.

   e. Tinjau dan terima Saya mengakui bahwa Acara Siklus Hidup Grup akan diaktifkan untuk membuat pemberitahuan sinkronisasi tag. GLE memungkinkan AWS untuk melihat perubahan pada sumber daya yang ditandai dengan pasangan nilai kunci Anda.
3. Pilih Berikutnya.
4. Tinjau detail aplikasi Anda, pasangan nilai kunci tag yang dipilih, dan pratinjau sumber daya yang akan ditambahkan ke aplikasi.

> **Note**
>
> Secara default, membuat aplikasi menggunakan pasangan nilai kunci tag yang ada menciptakan sinkronisasi tag. Setelah penyiapan, tag-sync juga terus mengelola sumber daya aplikasi, menambahkan atau menghapus sumber daya saat diberi tag atau tidak ditandai dengan pasangan kunci-nilai yang ditentukan. Anda dapat mengelola sinkronisasi tag dari halaman Kelola sumber daya aplikasi.

10. Jika mengaitkan CloudFormation tumpukan, pilih kotak centang di bagian bawah halaman.

> **Note**
>
> Menambahkan CloudFormation tumpukan ke aplikasi memerlukan pembaruan tumpukan karena semua sumber daya yang ditambahkan ke aplikasi Anda ditandai dengan tag

AWS aplikasi. Konfigurasi manual yang dilakukan setelah tumpukan terakhir diperbarui mungkin tidak tercermin setelah pembaruan ini. Hal ini dapat menyebabkan downtime atau masalah aplikasi lainnya. Untuk informasi selengkapnya, lihat Memperbarui perilaku sumber daya tumpukan di Panduan CloudFormation Pengguna.

11. Pilih Create application (Buat aplikasi).

## Onboard AppRegistry Aplikasi yang ada di MyApplications

Anda dapat menggunakan AppRegistry aplikasi yang sudah ada yang dibuat sebelum 8 November 2023 untuk memulai dengan MyApplications.

Untuk onboard aplikasi yang ada AppRegistry

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah sisi kiri, pilih MyApplications.
3. Gunakan bilah pencarian untuk menemukan aplikasi Anda.
4. Pilih aplikasi Anda.
5. Pilih Onboard ***application name***.
6. Jika mengaitkan CloudFormation tumpukan, pilih kotak centang di kotak peringatan.
7. Pilih aplikasi Onboard.

## Melihat aplikasi di MyApplications

Anda dapat melihat aplikasi Anda dari MyApplications atau menu Layanan. Jika melihat aplikasi Anda dari MyApplications, Anda dapat melihatnya di semua Wilayah AWS atau spesifik Wilayah AWS dan informasi yang relevan dalam tampilan kartu atau tabel.

**Note**

Anda juga dapat melihat aplikasi yang ditambahkan ke Favorit Anda dari menu favorit. Untuk informasi selengkapnya, lihat Favorit di Konsol Manajemen AWS.

myApplications

Untuk melihat aplikasi di MyApplications

1. Buka Konsol Manajemen AWS.
2. Di bilah sisi kiri, pilih MyApplications.
3. Di Wilayah, pilih Wilayah Saat Ini atau Wilayah yang Didukung.
4. Untuk menemukan aplikasi tertentu, masukkan nama, kata kunci, atau deskripsi di bilah pencarian.
5. (Opsional) Tampilan default Anda adalah tampilan kartu. Untuk menyesuaikan halaman aplikasi Anda:
    a. Pilih ikon roda gigi.
    b. (Opsional) Pilih ukuran halaman Anda.
    c. (Opsional) Pilih tampilan kartu atau tabel.
    d. (Opsional) Pilih ukuran halaman Anda.
    e. (Opsional) Jika menggunakan tampilan tabel, pilih properti untuk tampilan tabel Anda.
    f. (Opsional) Alihkan properti aplikasi apa yang terlihat dan urutan kemunculannya.
    g. Pilih Konfirmasi.

Services menu

Untuk melihat aplikasi dari menu Layanan

1. Buka Konsol Manajemen AWS.
2. Di bilah navigasi, pilih Layanan ().
3. Pilih Semua aplikasi.
4. Pilih aplikasi.
5. (Opsional) Pilih tampilan.
6. (Opsional) Pilih filter. Anda dapat memfilter sumber daya Anda berdasarkan Properti atau Tag. Untuk informasi selengkapnya, lihat Referensi sintaks kueri penelusuran untuk Resource Explorer di Panduan Penjelajah Sumber Daya AWS Pengguna.
7. (Opsional) Pilih sumber daya untuk melihatnya di konsol layanan yang relevan.

> **Tip**
>
> Anda dapat melanjutkan penelusuran sumber daya yang Anda tinggalkan dengan memilih Layanan (). Filter pencarian yang Anda terapkan juga akan bertahan.

## Mengedit aplikasi di MyApplications

Mengedit aplikasi Anda terbuka AppRegistry sehingga Anda dapat memperbarui deskripsinya. Anda juga dapat menggunakan AppRegistry untuk mengedit tag dan grup atribut aplikasi Anda.

Untuk mengedit aplikasi

1. Buka Konsol Manajemen AWS.
2. Di bilah sisi kiri konsol, pilih MyApplications.
3. Pilih aplikasi yang ingin Anda edit.
4. Di dasbor MyApplication, pilih Actions dan kemudian pilih Edit aplikasi.
5. Dalam aplikasi Edit, buat perubahan yang Anda inginkan pada deskripsi, tag, dan grup atribut aplikasi Anda.

   > **Note**
   >
   > Untuk informasi selengkapnya tentang mengelola tag dan grup atribut, lihat Mengelola tag dan Mengedit grup atribut di Panduan AWS Service Catalog AppRegistry Administrator.

6. Pilih Perbarui.

## Menghapus aplikasi di MyApplications

Anda dapat menghapus aplikasi jika tidak lagi diperlukan. Sebelum menghapus aplikasi, pastikan Anda menghapus semua pembagian sumber daya terkait dan grup atribut yang tidak dibuat oleh AWS layanan.

> **Note**
>
> Menghapus aplikasi tidak memengaruhi sumber daya Anda. Sumber daya yang ditandai dengan tag AWS aplikasi akan tetap ditandai.

Untuk menghapus aplikasi

1. Buka Konsol Manajemen AWS.
2. Di bilah sisi kiri konsol, pilih MyApplications.
3. Pilih aplikasi yang ingin Anda hapus.
4. Di dasbor MyApplication, pilih Actions.
5. Pilih Hapus aplikasi.
6. Konfirmasikan penghapusan Anda, lalu pilih Hapus.

## Membuat cuplikan kode di MyApplications

MyApplications membuat cuplikan kode untuk semua aplikasi Anda. Anda dapat menggunakan cuplikan kode untuk secara otomatis menambahkan sumber daya yang baru dibuat ke aplikasi menggunakan alat Infrastructure as Code (IAc). Semua sumber daya yang ditambahkan ditandai dengan tag AWS aplikasi untuk mengaitkannya dengan aplikasi Anda.

Untuk membuat cuplikan kode untuk aplikasi Anda

1. Buka Konsol Manajemen AWS.
2. Di bilah sisi kiri konsol, pilih MyApplications.
3. Cari dan pilih aplikasi.
4. Pilih Tindakan.
5. Pilih Dapatkan cuplikan kode.
6. Pilih jenis cuplikan kode.
7. Pilih Salin untuk menyalin kode ke clipboard Anda.
8. Tempelkan kode Anda ke alat IAC Anda.

# Sumber daya di MyApplications

Di AWS, sumber daya adalah entitas yang dapat Anda gunakan. Contohnya termasuk instans Amazon EC2, AWS CloudFormation tumpukan, atau bucket Amazon S3. Anda dapat mengelola sumber daya Anda di MyApplications dengan menambahkan dan menghapusnya dari aplikasi.

Topik


- Menambahkan sumber daya di MyApplications
- Menghapus sumber daya di MyApplications
- Melihat sumber daya di MyApplications


## Menambahkan sumber daya di MyApplications

Menambahkan sumber daya ke aplikasi Anda memungkinkan Anda mengelompokkannya dan mengelola keamanan, kinerja, dan kepatuhan mereka. Anda dapat menambahkan sumber daya ke aplikasi yang ada dengan mencarinya dan memilihnya atau dengan menggunakan tag yang ada dan melakukan sinkronisasi tag.

Search and select resources

Untuk mencari dan memilih sumber daya

1. Buka Konsol Manajemen AWS.
2. Di bilah sisi kiri konsol, pilih MyApplications.
3. Cari dan pilih aplikasi.
4. Pilih Kelola sumber daya.
5. Pilih Tambahkan sumber daya.
6. (Opsional) Pilih tampilan.
7. Cari sumber daya Anda. Anda dapat mencari berdasarkan kata kunci, nama atau jenis, atau memilih jenis sumber daya.

> **Note**
>
> Jika Anda tidak dapat menemukan sumber daya yang Anda cari, pecahkan masalah dengan. Penjelajah Sumber Daya AWS Untuk informasi selengkapnya, lihat

Memecahkan masalah penelusuran Resource Explorer di Panduan Pengguna Resource Explorer.

8. Pilih kotak centang di sebelah sumber daya yang ingin Anda tambahkan.
9. Pilih Tambahkan.

Automatically add resources using tags

Saat membuat aplikasi, Anda dapat mengumpulkan sumber daya secara massal dengan menentukan pasangan nilai kunci tag yang ada. Dengan metode ini, AWS secara otomatis menerapkan `awsApplication` tag ke semua sumber daya, dan membuat sinkronisasi tag untuk sumber daya aplikasi secara default. Dengan sinkronisasi tag diaktifkan, sumber daya apa pun yang ditandai dengan pasangan nilai kunci tag yang ditentukan secara otomatis ditambahkan ke aplikasi.

Untuk menambahkan sumber daya menggunakan tag yang ada

1. Buka Konsol Manajemen AWS.
2. Di bilah sisi kiri konsol, pilih MyApplications.
3. Pilih Kelola sumber daya.
4. Pilih Buat sinkronisasi tag.
5. Pilih kunci dan nilai tag yang ada:
    a. Pilih Peran yang digunakan untuk menandai sumber daya. Untuk informasi selengkapnya, lihat Izin tugas sinkronisasi Tag yang diperlukan di Panduan Administrator AWS Service Catalog AppRegistry .
    b. Pilih tombol Tag.
    c. Pilih nilai Tag.
    d. Tinjau dan terima Saya mengakui bahwa Acara Siklus Hidup Grup akan diaktifkan untuk membuat pemberitahuan sinkronisasi tag. GLE memungkinkan AWS untuk melihat perubahan pada sumber daya yang ditandai dengan pasangan nilai kunci Anda.
6. Pilih Buat sinkronisasi tag.

Menyelesaikan kesalahan sinkronisasi tag di MyApplications

Bagian ini menjelaskan kesalahan sinkronisasi tag umum dan cara mengatasinya. Setelah mencoba mengatasi kesalahan, Anda dapat mencoba lagi tugas sinkronisasi tag yang gagal.

- Izin tidak memadai — Anda tidak memiliki izin minimum yang diperlukan untuk memulai, memperbarui, atau membatalkan sinkronisasi tanda. Tinjau izin yang diperlukan sinkronisasi Tag untuk informasi selengkapnya. Setelah memastikan peran yang Anda tentukan untuk melakukan sinkronisasi tag memiliki izin minimum yang diperlukan, coba lagi tugas sinkronisasi tag yang gagal.
- Sudah ada — Tugas dengan pasangan kunci-nilai tanda ini sudah ada untuk aplikasi ini. Aplikasi dapat mendukung lebih dari satu sinkronisasi tanda, tetapi setiap sinkronisasi tanda harus memiliki pasangan kunci-nilai tanda yang berbeda. Setelah Anda menentukan pasangan kunci-nilai tanda yang berbeda, coba lagi tugas sinkronisasi tanda yang gagal.
- Batas maksimum tercapai — Anda telah mencapai maksimum 100 tugas sinkronisasi tanda per akun, di semua aplikasi.

## Menghapus sumber daya di MyApplications

Anda dapat menghapus sumber daya untuk memisahkannya dari aplikasi Anda.

Untuk menghapus sumber daya

1. Buka Konsol Manajemen AWS.
2. Di bilah sisi kiri konsol, pilih MyApplications.
3. Cari dan pilih aplikasi.
4. Pilih Kelola sumber daya.
5. (Opsional) Pilih tampilan.
6. Cari sumber daya Anda. Anda dapat mencari berdasarkan kata kunci, nama atau jenis, atau memilih jenis sumber daya.

> **Note**
>
> Jika Anda tidak dapat menemukan sumber daya yang Anda cari, pecahkan masalah dengan. Penjelajah Sumber Daya AWS Untuk informasi selengkapnya, lihat

Memecahkan masalah penelusuran Resource Explorer di Panduan Pengguna Resource Explorer.

7. Pilih Hapus.
8. Konfirmasikan bahwa Anda ingin menghapus sumber daya dengan memilih Hapus sumber daya.

## Melihat sumber daya di MyApplications

Anda dapat melihat sumber daya aplikasi Anda dari MyApplications dan menu Layanan.

myApplications

Untuk melihat sumber daya Anda di MyApplications

1. Buka Konsol Manajemen AWS.
2. Perluas sidebar kiri dan pilih MyApplications.
3. Pilih aplikasi.
4. Di widget Sumber Daya, lihat sumber daya Anda.

Services menu

Untuk melihat aplikasi dari menu Layanan

1. Buka Konsol Manajemen AWS.
2. Di bilah navigasi, pilih Layanan ().
3. Pilih Semua aplikasi.
4. Pilih aplikasi.
5. (Opsional) Pilih tampilan.
6. (Opsional) Pilih filter. Anda dapat memfilter sumber daya Anda berdasarkan Properti atau Tag. Untuk informasi selengkapnya, lihat Referensi sintaks kueri penelusuran untuk Resource Explorer di Panduan Penjelajah Sumber Daya AWS Pengguna.
7. (Opsional) Pilih sumber daya untuk melihatnya di konsol layanan yang relevan.

> **Tip**
>
> Anda dapat melanjutkan penelusuran sumber daya yang Anda tinggalkan dengan memilih Layanan (). Filter pencarian yang Anda terapkan juga akan bertahan.

## Dasbor MyApplications di AWS Console Home

Setiap aplikasi yang Anda buat atau onboard memiliki dasbor MyApplications sendiri. Dasbor MyApplications berisi biaya, keamanan, dan widget operasional yang memunculkan wawasan dari berbagai layanan. AWS Setiap widget juga dapat difavoritkan, disusun ulang, dihapus, atau diubah ukurannya. Untuk informasi selengkapnya, lihat Bekerja dengan widget di AWS Console Home.

Topik


- Widget pengaturan dasbor aplikasi
- Widget ringkasan aplikasi
- Widget komputasi
- Widget biaya dan penggunaan
- AWS Widget keamanan
- AWS Widget ketahanan
- Widget sumber daya
- DevOps widget
- Widget pemantauan dan operasi
- Tag widget


### Widget pengaturan dasbor aplikasi

Widget ini berisi daftar aktivitas memulai yang disarankan yang dapat Anda gunakan untuk membantu Anda mengonfigurasi Layanan AWS pengelolaan sumber daya aplikasi.

### Widget ringkasan aplikasi

Widget ini menunjukkan nama, deskripsi, dan tag AWS aplikasi untuk aplikasi Anda. Anda dapat mengakses dan menyalin tag aplikasi di Infrastructure as Code (IAC) untuk menandai sumber daya secara manual.

## Widget komputasi

Widget ini menampilkan informasi dan metrik untuk sumber daya komputasi, yang Anda tambahkan ke aplikasi Anda. Ini termasuk alarm total dan total jenis sumber daya komputasi. Widget ini juga menampilkan bagan tren metrik kinerja sumber daya dari Amazon CloudWatch untuk pemanfaatan CPU instans Amazon EC2 dan pemanggilan Lambda.

### Mengkonfigurasi widget Compute

Untuk mengisi data di widget Compute, siapkan setidaknya satu instans Amazon EC2 atau fungsi Lambda untuk aplikasi Anda. Untuk informasi selengkapnya, lihat Dokumentasi Amazon Elastic Compute Cloud dan Memulai Lambda di Panduan AWS Lambda Pengembang.

## Widget biaya dan penggunaan

Widget ini menampilkan data AWS biaya dan penggunaan untuk sumber daya aplikasi Anda. Anda dapat menggunakan data ini untuk membandingkan biaya bulanan dan melihat rincian biaya berdasarkan. Layanan AWS Widget ini hanya merangkum biaya untuk sumber daya yang ditandai dengan tag AWS aplikasi, tidak termasuk pajak, biaya, dan biaya bersama lainnya yang tidak terkait langsung dengan sumber daya. Biaya yang ditampilkan tidak tercampur dan diperbarui setidaknya sekali setiap 24 jam. FOr informasi selengkapnya, lihat Menganalisis biaya Anda dengan Penjelajah Sumber Daya AWS di Panduan AWS Cost Management Pengguna.

### Mengkonfigurasi widget Biaya dan penggunaan

Untuk mengonfigurasi widget Biaya dan penggunaan, aktifkan AWS Cost Explorer Service aplikasi dan akun Anda. Layanan ini ditawarkan tanpa biaya tambahan dan tidak ada biaya pengaturan atau komitmen di muka. Untuk informasi selengkapnya, lihat Mengaktifkan Cost Explorer di Panduan AWS Cost Management Pengguna.

## AWS Widget keamanan

Widget ini menampilkan temuan keamanan dari AWS Keamanan untuk aplikasi Anda. AWS Keamanan memberikan pandangan komprehensif tentang temuan keamanan untuk aplikasi Anda di AWS. Anda dapat mengakses temuan prioritas terbaru berdasarkan tingkat keparahan, memantau postur keamanannya, mengakses temuan kritis atau tingkat keparahan tinggi baru-baru ini, dan mendapatkan wawasan untuk langkah selanjutnya. Untuk informasi selengkapnya, lihat AWS Security Hub CSPM.

Mengkonfigurasi widget AWS Keamanan

Untuk mengonfigurasi widget AWS Keamanan, AWS Security Hub CSPM siapkan aplikasi dan akun Anda. Untuk informasi lebih lanjut, lihat Apa itu AWS Security Hub CSPM? dalam AWS Security Hub CSPM User Guide. Untuk informasi harga, lihat uji coba AWS Security Hub CSPM gratis, penggunaan, dan harga di Panduan AWS Security Hub CSPM Pengguna.

AWS Security Hub CSPM mengharuskan Anda untuk mengkonfigurasi AWS Config Recording. Layanan ini memberikan tampilan terperinci tentang sumber daya yang terkait dengan AWS akun Anda. Untuk informasi selengkapnya, lihat AWS Systems Manager di AWS Systems Manager Panduan Pengguna.

## AWS Widget ketahanan

Widget ini menampilkan detail ketahanan dari AWS Resilience Hub untuk aplikasi Anda. Setelah memulai penilaian, AWS Resiliency Hub menganalisis postur ketahanan aplikasi Anda dengan mengevaluasi sumber daya mereka terhadap kebijakan ketahanan yang telah ditentukan sebelumnya. Anda dapat mengakses metrik seperti skor ketahanan, pelanggaran kebijakan, penyimpangan kebijakan, penyimpangan sumber daya, dan riwayat skor ketahanan Anda. Aplikasi Anda dinilai setiap hari untuk pelacakan yang disempurnakan, tetapi Anda dapat menonaktifkannya kapan saja. Untuk informasi selengkapnya, lihat AWS Resilience Hub. Untuk informasi harga, lihat Harga AWS Resilience Hub.

Mengkonfigurasi widget AWS Ketahanan

Untuk mengkonfigurasi widget AWS Resiliency, tambahkan aplikasi. Untuk informasi lebih lanjut, lihat Apa itu AWS Resilience Hub? dalam AWS Resilience Hub User Guide.

## Widget sumber daya

Widget ini menggunakan AWS Resource Explorer untuk menampilkan sumber daya yang telah Anda tambahkan ke aplikasi Anda dalam tampilan. Anda juga dapat menggunakan widget ini untuk mencari atau memfilter sumber daya Anda menggunakan metadata sumber daya seperti nama, tag, dan. IDs Untuk informasi selengkapnya, lihat AWS Resource Explorer.

Mengkonfigurasi widget Sumber Daya

Untuk mengkonfigurasi widget sumber daya, onboard dengan Resource Explorer. Untuk informasi selengkapnya, lihat Memulai Resource Explorer di Panduan Pengguna AWS Resource Explorer.

## DevOps widget

Widget ini menampilkan wawasan operasional sehingga Anda dapat menilai kepatuhan dan mengambil tindakan untuk aplikasi Anda. Wawasan ini meliputi:

- Manajemen armada
- Manajemen negara
- Manajemen tambalan
- Konfigurasi dan OpsItems manajemen

### Mengkonfigurasi widget DevOps

Untuk mengkonfigurasi DevOps widget, aktifkan AWS Systems Manager OpsCenter aplikasi dan akun Anda. Untuk informasi selengkapnya, lihat Memulai Systems Manager Explorer dan OpsCenter di Panduan AWS Systems Manager Pengguna. Mengaktifkan OpsCenter memungkinkan AWS Systems Manager Explorer untuk mengkonfigurasi AWS Config dan Amazon CloudWatch agar acara mereka secara otomatis dibuat OpsItems berdasarkan aturan dan peristiwa yang umum digunakan. Untuk informasi selengkapnya, lihat Mengatur OpsCenter di Panduan AWS Systems Manager Pengguna.

Anda dapat mengonfigurasi instans agar agen Systems Manager dapat dijalankan dan menerapkan izin untuk mengaktifkan pemindaian tambalan. Untuk informasi selengkapnya, lihat Pengaturan AWS Systems Manager Cepat di Panduan AWS Systems Manager Pengguna.

Anda juga dapat mengatur penambalan otomatis instans Amazon EC2 untuk aplikasi Anda dengan menyiapkan AWS Systems Manager Patch Manager. Untuk informasi selengkapnya, lihat Menggunakan kebijakan patch Pengaturan Cepat di Panduan AWS Systems Manager Pengguna.

Untuk informasi harga, lihat Harga AWS Systems Manager.

## Widget pemantauan dan operasi

Widget ini menunjukkan:

- Alarm dan peringatan untuk sumber daya yang terkait dengan aplikasi Anda
- Tujuan tingkat layanan aplikasi (SLOs) dan metrik
- Metrik Sinyal AWS Aplikasi yang Tersedia

Mengkonfigurasi widget Pemantauan dan operasi

Untuk mengonfigurasi widget Pemantauan dan operasi, buat CloudWatch alarm dan kenari di akun Anda AWS . Untuk informasi selengkapnya, lihat Menggunakan CloudWatch alarm Amazon dan Membuat kenari di CloudWatch Panduan Pengguna Amazon. Untuk CloudWatch alarm dan harga kenari sintetis, lihat CloudWatch harga Amazon dan Blog Operasi dan Migrasi AWS Cloud masing-masing.

Untuk informasi selengkapnya tentang Sinyal CloudWatch Aplikasi, lihat Mengaktifkan Sinyal CloudWatch Aplikasi Amazon di Panduan CloudWatch Pengguna Amazon.

### Tag widget

Widget ini menampilkan semua tag yang terkait dengan aplikasi Anda. Anda dapat menggunakan widget ini untuk melacak dan mengelola metadata aplikasi (kekritisan, lingkungan, pusat biaya). Untuk informasi selengkapnya, lihat Apa itu tag? di Buku AWS Putih Praktik Terbaik untuk Menandai AWS Sumber Daya.

## Mengobrol dengan Pengembang Amazon Q di AWS Console Home

Amazon Q Developer adalah asisten percakapan yang didukung kecerdasan buatan (AI) generatif yang dapat membantu Anda memahami, membangun, memperluas, dan mengoperasikan AWS aplikasi. Anda dapat mengajukan pertanyaan tentang Amazon Q AWS, termasuk pertanyaan tentang AWS arsitektur, AWS sumber daya Anda, praktik terbaik, dokumentasi, dan banyak lagi. Anda juga dapat membuat kasus dukungan dan menerima bantuan dari agen langsung. Untuk informasi selengkapnya, lihat Apa itu Amazon Q? di Panduan Pengguna Pengembang Amazon Q.

### Memulai Amazon Q

Anda dapat mulai mengobrol dengan Amazon Q di situs web AWS Dokumentasi Konsol Manajemen AWS, situs AWS web, atau AWS Console Mobile Application dengan memilih ikon Amazon Q heksagonal. Untuk informasi selengkapnya, lihat Memulai Amazon Q Developer di Panduan Pengguna Pengembang Amazon Q.

### Contoh pertanyaan

Berikut adalah beberapa contoh pertanyaan yang dapat Anda tanyakan kepada Amazon Q:

- How do I get billing support?
- How do I create an EC2 instance?
- How do I troubleshoot a "Failed to load" error?
- How do I close an AWS account?
- Can you connect me with a person?

# Konsol Manajemen AWS Akses Pribadi

Konsol Manajemen AWS Private Access adalah fitur keamanan canggih untuk mengontrol akses ke Konsol Manajemen AWS. Akses Pribadi Konsol berguna saat Anda ingin mencegah pengguna masuk ke tak terduga Akun AWS dari dalam jaringan Anda. Dengan fitur ini, Anda dapat membatasi akses ke Konsol Manajemen AWS satu-satunya ke set tertentu yang diketahui Akun AWS ketika lalu lintas berasal dari dalam jaringan Anda. Console Private Access juga berguna ketika Anda ingin memastikan bahwa semua panggilan dari Konsol Manajemen AWS to Layanan AWS berasal dari dalam jaringan Anda dan dari akun yang diizinkan.

Topik


- Didukung Wilayah AWS, konsol layanan, dan fitur untuk Akses Pribadi
- Ikhtisar kontrol keamanan Akses Konsol Manajemen AWS Pribadi
- Titik akhir VPC dan konfigurasi DNS yang diperlukan
- Menerapkan kebijakan kontrol layanan dan kebijakan titik akhir VPC
- Menerapkan kebijakan berbasis identitas dan jenis kebijakan lainnya
- Coba Akses Konsol Manajemen AWS Pribadi
- Arsitektur referensi


## Didukung Wilayah AWS, konsol layanan, dan fitur untuk Akses Pribadi

Konsol Manajemen AWS Private Access hanya mendukung sebagian Wilayah dan AWS layanan. Konsol layanan yang tidak didukung akan tidak aktif di. Konsol Manajemen AWS Selain itu, Konsol Manajemen AWS fitur tertentu mungkin dinonaktifkan saat menggunakan Akses Konsol Manajemen AWS Pribadi, misalnya, pilihan Wilayah Default di Pengaturan Terpadu.

Wilayah dan konsol layanan berikut didukung.

Wilayah yang Didukung

- AS Timur (Ohio)
- AS Timur (Virginia Utara)
- AS Barat (California Utara)

- AS Barat (Oregon)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Seoul)
- Asia Pasifik (Osaka)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Malaysia)
- Asia Pasifik (Thailand)
- Asia Pasifik (Tokyo)
- Kanada (Pusat)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Paris)
- Eropa (Stockholm)
- Amerika Selatan (Sao Paulo)
- Africa (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Jakarta)
- Asia Pacific (Melbourne)
- Kanada Barat (Calgary)
- Meksiko (Tengah)
- Europe (Milan)
- Eropa (Spanyol)
- Eropa (Zürich)
- Timur Tengah (Bahrain)
- Middle East (UAE)
- Israel (Tel Aviv)

## Konsol layanan yang didukung

- Amazon API Gateway
- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- AWS Manajemen Penagihan dan Biaya
- AWS Budgets
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home

- AWS Control Tower
- Amazon DataZone
- AWS Database Migration Service
- AWS DataSync
- AWS DeepRacer
- AWS Direct Connect
- AWS Directory Service
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Tampilan Global Amazon EC2
- EC2 Image Builder
- Connect Instans Amazon EC2
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- AWS Firewall Manager
- GameLift Server Amazon
- AWS Glue
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty

- AWS IAM Identity Center
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Layanan Terkelola Amazon untuk Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Macie
- Amazon Managed Streaming untuk Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- Rekomendasi Strategi AWS Migration Hub
- Amazon MQ
- Penganalisis Akses Jaringan
- AWS Network Firewall
- AWS Network Manager
- OpenSearch Layanan Amazon
- AWS Organizations
- AWS Private Certificate Authority
- Dasbor Kesehatan Masyarakat
- Amazon Rekognition
- Amazon Relational Database Service

- AWS Resource Access Manager
- AWS Resource Groups dan Editor Tag
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver Firewall DNS
- Amazon S3 on Outposts
- Amazon SageMaker
- SageMaker Runtime Amazon
- Data Sintetis Amazon SageMaker AI
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub CSPM
- Service Quotas
- AWS Signer
- Layanan Email Sederhana Amazon
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- Dukungan
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- Pengaturan Terpadu
- Pengelola Alamat IP Amazon VPC
- Amazon Virtual Private Cloud
- Klien Amazon WorkSpaces Thin

# Ikhtisar kontrol keamanan Akses Konsol Manajemen AWS Pribadi

## Pembatasan akun Konsol Manajemen AWS dari jaringan Anda

Konsol Manajemen AWS Akses Pribadi berguna dalam skenario ketika Anda ingin membatasi akses ke Konsol Manajemen AWS dari jaringan Anda hanya ke kumpulan tertentu yang diketahui Akun AWS di organisasi Anda. Dengan demikian, Anda dapat mencegah pengguna masuk ke tak terduga Akun AWS dari dalam jaringan Anda. Anda dapat menerapkan kontrol ini menggunakan kebijakan titik akhir Konsol Manajemen AWS VPC. Untuk informasi selengkapnya, lihat Menerapkan kebijakan kontrol layanan dan kebijakan titik akhir VPC.

## Konektivitas dari jaringan Anda ke internet

Konektivitas internet dari jaringan Anda masih diperlukan untuk mengakses aset yang digunakan oleh Konsol Manajemen AWS, seperti konten statis (JavaScript, CSS, gambar), dan semua yang Layanan AWS tidak diaktifkan oleh AWS PrivateLink. Untuk daftar domain tingkat atas yang digunakan oleh Konsol Manajemen AWS, lihat. Pemecahan Masalah

> **Note**
>
> Saat ini, Konsol Manajemen AWS Private Access tidak mendukung endpoint seperti`status.aws.amazon.com`,`health.aws.amazon.com`, dan`docs.aws.amazon.com`. Anda perlu merutekan domain ini ke internet publik.

# Titik akhir VPC dan konfigurasi DNS yang diperlukan

Konsol Manajemen AWS Akses Pribadi memerlukan dua titik akhir VPC berikut per Wilayah. Ganti *`region`* dengan informasi Wilayah Anda sendiri.

1. com.amazonaws. *`region`*.console untuk Konsol Manajemen AWS
2. com.amazonaws. *`region`*.signin untuk AWS Sign-In

> **Note**
>
> Selalu menyediakan infrastruktur dan konektivitas jaringan ke Wilayah AS Timur (Virginia N.) (us-east-1), terlepas dari Wilayah lain yang Anda gunakan dengan. Konsol Manajemen AWS

Anda dapat menggunakan AWS Transit Gateway untuk mengatur konektivitas antara AS Timur (Virginia N.) dan setiap Wilayah lainnya. Untuk informasi selengkapnya, lihat Memulai gateway transit di panduan Gerbang Transit VPC Amazon. Anda juga dapat menggunakan peering VPC Amazon. Untuk informasi selengkapnya, lihat Apa itu mengintip VPC di Panduan Peering VPC Amazon. Untuk membandingkan opsi ini, lihat opsi konektivitas Amazon VPC-to-Amazon VPC di whitepaper Opsi Konektivitas Amazon Virtual Private Cloud.

Topik


- DNSkonfigurasi untuk Konsol Manajemen AWS dan AWS Sign-In
- Titik akhir VPC dan DNS konfigurasi untuk AWS layanan di Konsol Manajemen AWS


## DNSkonfigurasi untuk Konsol Manajemen AWS dan AWS Sign-In

Untuk merutekan lalu lintas jaringan Anda ke titik akhir VPC masing-masing, konfigurasikan DNS catatan di jaringan tempat pengguna Anda akan mengakses file. Konsol Manajemen AWSDNSCatatan ini akan mengarahkan lalu lintas browser pengguna Anda ke titik akhir VPC yang Anda buat.

Anda dapat membuat satu zona yang dihosting. Namun, titik akhir seperti `health.aws.amazon.com` dan tidak `docs.aws.amazon.com` akan dapat diakses karena tidak memiliki titik akhir VPC. Anda perlu merutekan domain ini ke internet publik. Kami menyarankan Anda membuat dua zona host pribadi per Wilayah, satu untuk `signin.aws.amazon.com` dan satu untuk `console.aws.amazon.com` dengan CNAME catatan berikut:

- Masuk
  - *region*.signin.aws.amazon.com menunjuk ke titik akhir AWS Sign-In VPC di zona masuk di mana Wilayah yang diinginkan DNS *region*
  - signin.aws.amazon.com menunjuk ke titik akhir VPC AWS Masuk di AS Timur (Virginia Utara) (us-east-1)
- Konsol
  - *region*.console.aws.amazon.com menunjuk ke titik akhir Konsol Manajemen AWS VPC di zona konsol di mana Wilayah yang diinginkan DNS *region*
  - *. *region*.console.aws.amazon.com menunjuk ke titik akhir Konsol Manajemen AWS VPC di zona konsol di mana Wilayah yang diinginkan DNS *region*

- *. *region*.console.aws.amazon.com menunjuk ke titik akhir VPC di zona konsol Konsol Manajemen AWS DNS
- CNAMECatatan tanpa wilayah hanya untuk Wilayah AS Timur (Virginia N.). Anda harus selalu mengatur Wilayah AS Timur (Virginia N.).
  - signin.aws.amazon.com menunjuk ke titik akhir AWS Sign-In VPC di AS Timur (Virginia Utara) (us-east-1)
  - *.console.aws.amazon.com menunjuk ke titik akhir Konsol Manajemen AWS VPC di AS Timur (Virginia Utara) (us-east-1)

Untuk petunjuk cara membuat CNAME rekaman, lihat Bekerja dengan catatan di Panduan Pengembang Amazon Route 53.

Beberapa AWS konsol, termasuk Amazon S3, menggunakan pola yang berbeda untuk DNS nama mereka. Berikut ini adalah dua contoh:

- support.console.aws.amazon.com
- s3.console.aws.amazon.com

Untuk dapat mengarahkan lalu lintas ini ke titik akhir Konsol Manajemen AWS VPC Anda, Anda perlu menambahkan nama-nama itu satu per satu. Kami menyarankan Anda mengonfigurasi perutean untuk semua titik akhir untuk pengalaman yang sepenuhnya pribadi. Namun, ini tidak diperlukan untuk menggunakan Akses Konsol Manajemen AWS Pribadi.

`json`File berikut berisi daftar lengkap titik akhir Layanan AWS s dan konsol untuk dikonfigurasi per Wilayah. Gunakan `PrivateIpv4DnsNames` bidang di bawah `com.amazonaws.`*`region`*`.console` titik akhir untuk DNS nama.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-tenggara 1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-tenggara 2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-selatan-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-selatan-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json

- https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

> **Note**
>
> Daftar ini diperbarui setiap bulan saat kami menambahkan titik akhir tambahan ke ruang lingkup Akses Konsol Manajemen AWS Pribadi. Untuk menjaga zona host pribadi Anda diperbarui, tarik daftar file sebelumnya secara berkala.

Jika Anda menggunakan Route 53 untuk mengonfigurasiDNS, buka https://console.aws.amazon.com/route53/ v2/hostedzones# untuk memverifikasi pengaturan. DNS Untuk setiap Zona Dihosting Pribadi di Rute 53, verifikasi bahwa kumpulan rekaman berikut ada.

- console.aws.amazon.com
- signin.aws.amazon.com
- *. *region*.console.aws.amazon.com
- *region*.console.aws.amazon.com
- *. *region*.console.aws.amazon.com
- signin.aws.amazon.com
- *region*.signin.aws.amazon.com
- Catatan tambahan hadir dalam file JSON yang terdaftar sebelumnya

## Titik akhir VPC dan DNS konfigurasi untuk AWS layanan di Konsol Manajemen AWS

Konsol Manajemen AWS Panggilan Layanan AWS melalui kombinasi permintaan browser langsung dan permintaan yang diproksi oleh server web. Untuk mengarahkan lalu lintas ini ke titik akhir Konsol Manajemen AWS VPC Anda, Anda harus menambahkan titik akhir VPC dan mengonfigurasi untuk setiap layanan dependen. DNS AWS

jsonFile-file berikut mencantumkan AWS PrivateLink dukungan Layanan AWS yang tersedia untuk Anda gunakan. Jika layanan tidak terintegrasi dengan AWS PrivateLink, itu tidak termasuk dalam file-file ini.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-tenggara 1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-tenggara 2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-selatan-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-selatan-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

Gunakan `ServiceName` bidang untuk titik akhir VPC layanan terkait untuk ditambahkan ke VPC Anda.

> **Note**
>
> Kami memperbarui daftar ini setiap bulan karena kami menambahkan dukungan untuk Akses Konsol Manajemen AWS Pribadi ke lebih banyak konsol layanan. Agar tetap terkini, tarik daftar file sebelumnya secara berkala dan perbarui titik akhir VPC Anda.

# Menerapkan kebijakan kontrol layanan dan kebijakan titik akhir VPC

Anda dapat menggunakan kebijakan kontrol layanan (SCPs) dan kebijakan titik akhir VPC untuk Akses Konsol Manajemen AWS Pribadi untuk membatasi kumpulan akun yang diizinkan menggunakan Konsol Manajemen AWS dari dalam VPC dan jaringan lokal yang terhubung.

Topik

- Menggunakan Konsol Manajemen AWS Private Access dengan kebijakan kontrol AWS Organizations layanan
- Izinkan Konsol Manajemen AWS penggunaan hanya untuk akun dan organisasi yang diharapkan (identitas tepercaya)

## Menggunakan Konsol Manajemen AWS Private Access dengan kebijakan kontrol AWS Organizations layanan

Jika AWS organisasi Anda menggunakan kebijakan kontrol layanan (SCP) yang memungkinkan layanan tertentu, Anda `signin:*` harus menambahkan tindakan yang diizinkan. Izin ini diperlukan karena masuk ke Konsol Manajemen AWS melalui titik akhir VPC Akses Pribadi melakukan otorisasi IAM yang diblokir SCP tanpa izin. Sebagai contoh, kebijakan kontrol layanan berikut memungkinkan Amazon EC2 dan CloudWatch layanan untuk digunakan dalam organisasi, termasuk saat diakses menggunakan titik akhir Akses Konsol Manajemen AWS Pribadi.

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  },
  "Resource": "*"
}
```

Untuk informasi selengkapnya SCPs, lihat Kebijakan kontrol layanan (SCPs) di Panduan AWS Organizations Pengguna.

# Izinkan Konsol Manajemen AWS penggunaan hanya untuk akun dan organisasi yang diharapkan (identitas tepercaya)

Konsol Manajemen AWS dan AWS Sign-In mendukung kebijakan titik akhir VPC yang secara khusus mengontrol identitas akun yang masuk.

Tidak seperti kebijakan titik akhir VPC lainnya, kebijakan ini dievaluasi sebelum otentikasi. Akibatnya, secara khusus mengontrol login dan penggunaan sesi yang diautentikasi saja, dan bukan tindakan AWS khusus layanan apa pun yang dilakukan sesi. Misalnya, saat sesi mengakses konsol AWS layanan, seperti konsol Amazon EC2, kebijakan titik akhir VPC ini tidak akan dievaluasi terhadap tindakan Amazon EC2 yang diambil untuk menampilkan halaman tersebut. Sebaliknya, Anda dapat menggunakan kebijakan IAM yang terkait dengan Principal IAM yang masuk untuk mengontrol izinnya terhadap tindakan layanan. AWS

> **Note**
>
> Kebijakan titik akhir VPC untuk dan titik akhir Konsol Manajemen AWS SignIn VPC hanya mendukung sebagian rumusan kebijakan yang terbatas. Setiap `Principal` dan `Resource` harus diatur ke `*` dan `Action` harus salah satu `*` atau`signin:*`. Anda mengontrol akses ke titik akhir VPC menggunakan `aws:PrincipalOrgId` dan `aws:PrincipalAccount` tombol kondisi.

Kebijakan berikut direkomendasikan untuk titik akhir Konsol dan SignIn VPC.

Kebijakan titik akhir VPC ini memungkinkan login ke Akun AWS AWS organisasi tertentu dan memblokir proses masuk ke akun lain.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

Kebijakan titik akhir VPC ini membatasi proses masuk ke daftar spesifik Akun AWS dan memblokir proses masuk ke akun lain.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

Kebijakan yang membatasi Akun AWS atau organisasi pada titik akhir VPC Masuk Konsol Manajemen AWS dan Masuk dievaluasi pada saat login dan dievaluasi ulang secara berkala untuk sesi yang ada.

# Menerapkan kebijakan berbasis identitas dan jenis kebijakan lainnya

Anda mengelola akses AWS dengan membuat kebijakan dan melampirkannya ke identitas IAM (pengguna, grup pengguna, atau peran) atau sumber daya. AWS Halaman ini menjelaskan cara kerja kebijakan saat digunakan bersama dengan Akses Konsol Manajemen AWS Pribadi.

## Kunci konteks kondisi AWS global yang didukung

Konsol Manajemen AWS Akses Pribadi tidak mendukung `aws:SourceVpce` dan kunci konteks kondisi `aws:VpcSourceIp` AWS global. Sebagai gantinya, Anda dapat menggunakan kondisi `aws:SourceVpc` IAM dalam kebijakan Anda, saat menggunakan Akses Konsol Manajemen AWS Pribadi.

## Bagaimana Konsol Manajemen AWS Private Access bekerja dengan aws: SourceVpc

Bagian ini menjelaskan berbagai jalur jaringan yang Konsol Manajemen AWS dapat diambil oleh permintaan yang dihasilkan oleh Anda Layanan AWS. Secara umum, konsol AWS layanan diimplementasikan dengan campuran permintaan browser langsung dan permintaan yang diproksi oleh server Konsol Manajemen AWS web ke. Layanan AWS Implementasi ini dapat berubah tanpa pemberitahuan. Jika persyaratan keamanan Anda mencakup akses untuk Layanan AWS menggunakan titik akhir VPC, sebaiknya Anda mengonfigurasi titik akhir VPC untuk semua layanan yang ingin Anda gunakan dari VPC, baik secara langsung maupun melalui Akses Pribadi. Konsol Manajemen AWS Selain itu, Anda harus menggunakan kondisi `aws:SourceVpc` IAM dalam kebijakan Anda daripada `aws:SourceVpce` nilai tertentu dengan fitur Akses Konsol Manajemen AWS Pribadi. Bagian ini memberikan rincian tentang cara kerja jalur jaringan yang berbeda.

Setelah pengguna masuk Konsol Manajemen AWS, mereka membuat permintaan Layanan AWS melalui kombinasi permintaan browser langsung dan permintaan yang diproksi oleh server Konsol Manajemen AWS web ke AWS server. Misalnya, permintaan data CloudWatch grafik dibuat langsung dari browser. Sedangkan beberapa permintaan konsol AWS layanan, seperti Amazon S3, diproksi oleh server web ke Amazon S3.

Untuk permintaan browser langsung, menggunakan Akses Konsol Manajemen AWS Pribadi tidak mengubah apa pun. Seperti sebelumnya, permintaan mencapai layanan melalui jalur jaringan apa pun yang telah dikonfigurasi VPC untuk dijangkau. monitoring.region.amazonaws.com Jika VPC

dikonfigurasi dengan titik akhir VPC untukcom.amazonaws.region.monitoring, permintaan akan mencapai melalui CloudWatch titik akhir VPC tersebut. CloudWatch Jika tidak ada titik akhir VPC CloudWatch, permintaan akan mencapai CloudWatch titik akhir publiknya, melalui Internet Gateway di VPC. Permintaan yang tiba CloudWatch melalui titik akhir CloudWatch VPC akan memiliki kondisi IAM `aws:SourceVpc` dan `aws:SourceVpce` disetel ke nilainya masing-masing. Mereka yang mencapai CloudWatch melalui titik akhir publiknya akan `aws:SourceIp` mengatur ke alamat IP sumber permintaan. Untuk informasi selengkapnya tentang kunci kondisi IAM ini, lihat Kunci kondisi global di Panduan Pengguna IAM.

Untuk permintaan yang diproksi oleh server Konsol Manajemen AWS web, seperti permintaan yang dibuat konsol Amazon S3 untuk mencantumkan bucket Anda saat Anda mengunjungi konsol Amazon S3, jalur jaringannya berbeda. Permintaan ini tidak dimulai dari VPC Anda dan oleh karena itu jangan gunakan titik akhir VPC yang mungkin telah Anda konfigurasikan di VPC Anda untuk layanan tersebut. Bahkan jika Anda memiliki titik akhir VPC untuk Amazon S3 dalam kasus ini, permintaan sesi Anda ke Amazon S3 untuk membuat daftar bucket tidak menggunakan titik akhir VPC Amazon S3. Namun, saat Anda menggunakan Akses Konsol Manajemen AWS Pribadi dengan layanan yang didukung, permintaan ini (misalnya, ke Amazon S3) akan menyertakan kunci `aws:SourceVpc` kondisi dalam konteks permintaannya. Kunci `aws:SourceVpc` kondisi akan disetel ke ID VPC tempat titik akhir Akses Konsol Manajemen AWS Pribadi Anda untuk login dan konsol digunakan. Jadi, jika Anda menggunakan `aws:SourceVpc` batasan dalam kebijakan berbasis identitas, Anda harus menambahkan ID VPC VPC ini yang menghosting titik masuk dan konsol Akses Pribadi. Konsol Manajemen AWS `aws:SourceVpce`Kondisi akan disetel ke titik akhir IDs VPC login atau konsol masing-masing.

> **Note**
>
> Jika pengguna Anda memerlukan akses ke konsol layanan yang tidak didukung oleh Akses Konsol Manajemen AWS Pribadi, Anda harus menyertakan daftar alamat jaringan publik yang diharapkan (seperti rentang jaringan lokal) menggunakan kunci `aws:SourceIP` kondisi dalam kebijakan berbasis identitas pengguna.

## Bagaimana jalur jaringan yang berbeda tercermin dalam CloudTrail

Jalur jaringan yang berbeda yang digunakan oleh permintaan yang dihasilkan oleh Anda Konsol Manajemen AWS tercermin dalam riwayat CloudTrail acara Anda.

Untuk permintaan browser langsung, menggunakan Akses Konsol Manajemen AWS Pribadi tidak mengubah apa pun. CloudTrail event akan mencakup detail tentang koneksi, seperti ID titik akhir VPC yang digunakan untuk melakukan panggilan API layanan.

Untuk permintaan yang diproksi oleh server Konsol Manajemen AWS web, CloudTrail acara tidak akan menyertakan detail terkait VPC apa pun. Namun, permintaan awal AWS Sign-In yang diperlukan untuk membuat sesi browser, seperti jenis `AwsConsoleSignIn` acara, akan menyertakan ID titik akhir AWS Sign-In VPC dalam detail acara.

# Coba Akses Konsol Manajemen AWS Pribadi

Bagian ini menjelaskan cara mengatur dan menguji Akses Konsol Manajemen AWS Pribadi di akun baru.

Konsol Manajemen AWS Private Access adalah fitur keamanan canggih dan membutuhkan pengetahuan sebelumnya tentang jaringan dan pengaturan VPCs. Topik ini menjelaskan bagaimana Anda dapat mencoba Konsol Manajemen AWS Private Access tanpa infrastruktur skala penuh.

Topik

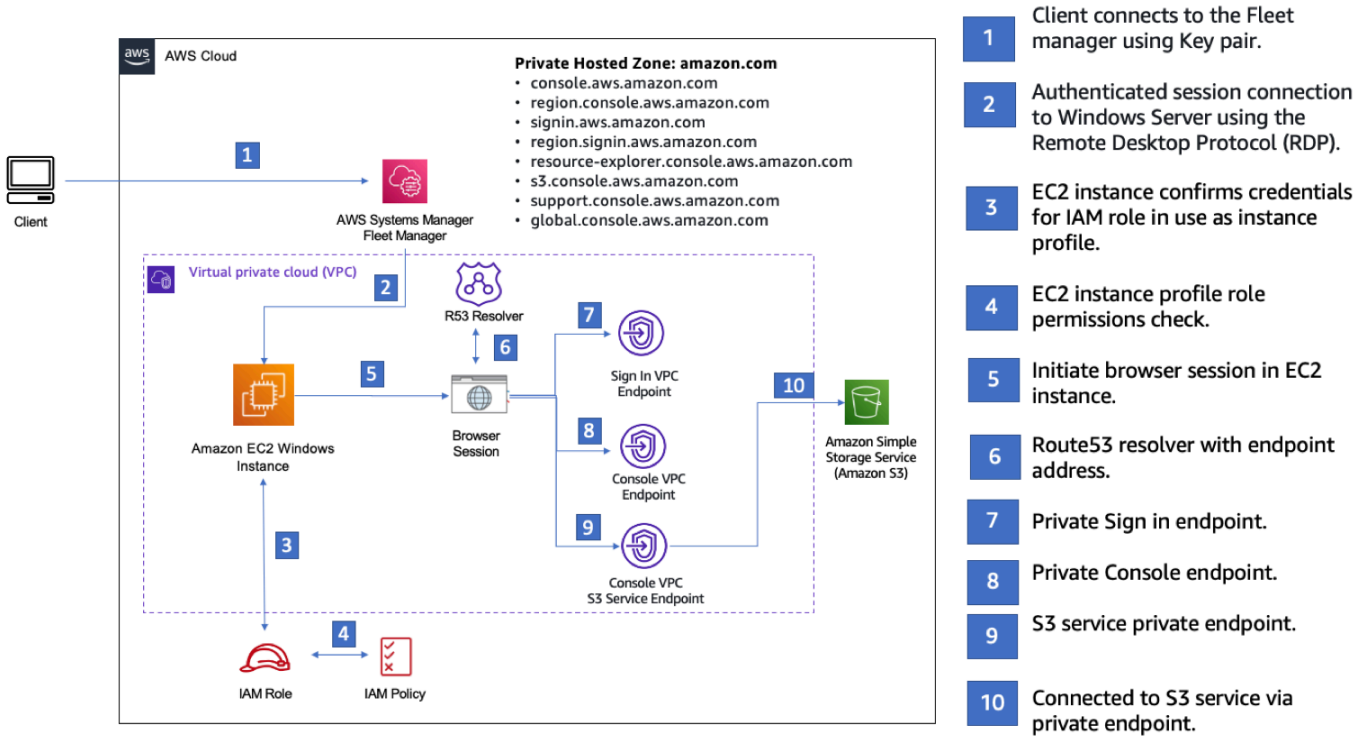
- Uji pengaturan dengan Amazon EC2
- Uji pengaturan dengan Amazon WorkSpaces
- Uji pengaturan VPC dengan kebijakan IAM

## Uji pengaturan dengan Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2), menyediakan kapasitas komputasi yang dapat diskalakan di cloud Amazon Web Services. Anda dapat menggunakan Amazon EC2 untuk meluncurkan server virtual sebanyak atau sesedikit yang Anda butuhkan, mengonfigurasi keamanan dan jaringan, serta mengelola penyimpanan. Dalam pengaturan ini, kami menggunakan Fleet Manager, kemampuan AWS Systems Manager, untuk terhubung ke instans Windows Amazon EC2 menggunakan Remote Desktop Protocol (RDP).

Panduan ini menunjukkan lingkungan pengujian untuk menyiapkan dan mengalami koneksi Akses Konsol Manajemen AWS Pribadi ke Amazon Simple Storage Service dari instans Amazon EC2. Tutorial ini digunakan CloudFormation untuk membuat dan mengkonfigurasi pengaturan jaringan yang akan digunakan oleh Amazon EC2 untuk memvisualisasikan fitur ini.

Diagram berikut menjelaskan alur kerja untuk menggunakan Amazon EC2 untuk mengakses penyiapan Akses Konsol Manajemen AWS Pribadi. Ini menunjukkan bagaimana pengguna terhubung ke Amazon S3 menggunakan titik akhir pribadi.




Salin CloudFormation template berikut dan simpan ke file yang akan Anda gunakan di langkah ketiga dari Untuk mengatur prosedur jaringan.

> **Note**
>
> CloudFormation Template ini menggunakan konfigurasi yang saat ini tidak didukung di Israel (Tel Aviv) Wilayah.

Konsol Manajemen AWS Template Amazon CloudFormation EC2 lingkungan Akses Pribadi

```
Description: |
  AWS Management Console Private Access.
Parameters:
  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
```

```
    Description: CIDR range for VPC

  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't3.medium'
```

```
Resources:

#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PublicSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet3CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
```

```
      Fn::Select:
        - 2
        - Fn::GetAZs: ""

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
```

```
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

########################
# Route Tables
########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PrivateSubnetRouteTableAssociation3:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetC

  PublicRouteTable:
```

```
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB

  PublicSubnetBRouteTableAssociation3:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetC


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
```

```
          CidrIp: !GetAtt AppVPC.CidrBlock

  EC2SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Default EC2 Instance SG
      VpcId: !Ref AppVPC

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceEc2messages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
```

```
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
    VpcId: !Ref AppVPC

VPCEndpointInterfaceSsmmessages:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
    VpcId: !Ref AppVPC

VPCEndpointInterfaceSignin:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
    VpcId: !Ref AppVPC

VPCEndpointInterfaceConsole:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
```

```
      VpcId: !Ref AppVPC

#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
```

```
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  WidgetProxyRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "*.widget.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
        HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      Type: A
```

```
 ConsoleRecordRegional:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: !Sub "${AWS::Region}.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleRecordRegionalMultiSession:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 SigninHostedZone:
   Type: "AWS::Route53::HostedZone"
   Properties:
     HostedZoneConfig:
       Comment: 'Signin VPC Endpoint Hosted Zone'
     Name: 'signin.aws.amazon.com'
     VPCs:
       -
         VPCId: !Ref AppVPC
         VPCRegion: !Ref "AWS::Region"

 SigninRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'SigninHostedZone'
     Name: 'signin.aws.amazon.com'
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
```

```
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# EC2 INSTANCE
#########################

  Ec2InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          -
            Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

  Ec2InstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Path: /
      Roles:
       - !Ref Ec2InstanceRole
```

```
  EC2WinInstance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: !Ref LatestWindowsAmiId
      IamInstanceProfile: !Ref Ec2InstanceProfile
      KeyName: !Ref Ec2KeyPair
      InstanceType:
        Ref: InstanceTypeParameter
      SubnetId: !Ref PrivateSubnetA
      SecurityGroupIds:
        - Ref: EC2SecurityGroup
      BlockDeviceMappings:
        - DeviceName: /dev/sda1
          Ebs:
            VolumeSize: 50
      Tags:
      - Key: "Name"
        Value: "Console VPCE test instance"
```

Untuk mengatur jaringan

1. Masuk ke akun manajemen untuk organisasi Anda dan buka CloudFormation konsol.
2. Pilih Buat tumpukan.
3. Pilih Dengan sumber daya baru (standar). Unggah file CloudFormation template yang sebelumnya Anda buat, dan pilih Berikutnya.
4. Masukkan nama untuk tumpukan, seperti**`PrivateConsoleNetworkForS3`**, lalu pilih Berikutnya.
5. Untuk VPC dan subnet, masukkan rentang CIDR IP pilihan Anda, atau gunakan nilai default yang disediakan. Jika Anda menggunakan nilai default, verifikasi bahwa nilai tersebut tidak tumpang tindih dengan sumber daya VPC yang ada di Anda. Akun AWS
6. Untuk KeyPair parameter Ec2, pilih salah satu dari pasangan kunci Amazon EC2 yang ada di akun Anda. Jika Anda tidak memiliki key pair Amazon EC2 yang sudah ada, Anda harus membuatnya sebelum melanjutkan ke langkah berikutnya. Untuk informasi selengkapnya, lihat Membuat key pair menggunakan Amazon EC2 di Panduan Pengguna Amazon EC2.
7. Pilih Buat tumpukan.
8. Setelah tumpukan dibuat, pilih tab Resources untuk melihat sumber daya yang telah dibuat.

Untuk terhubung ke instans Amazon EC2

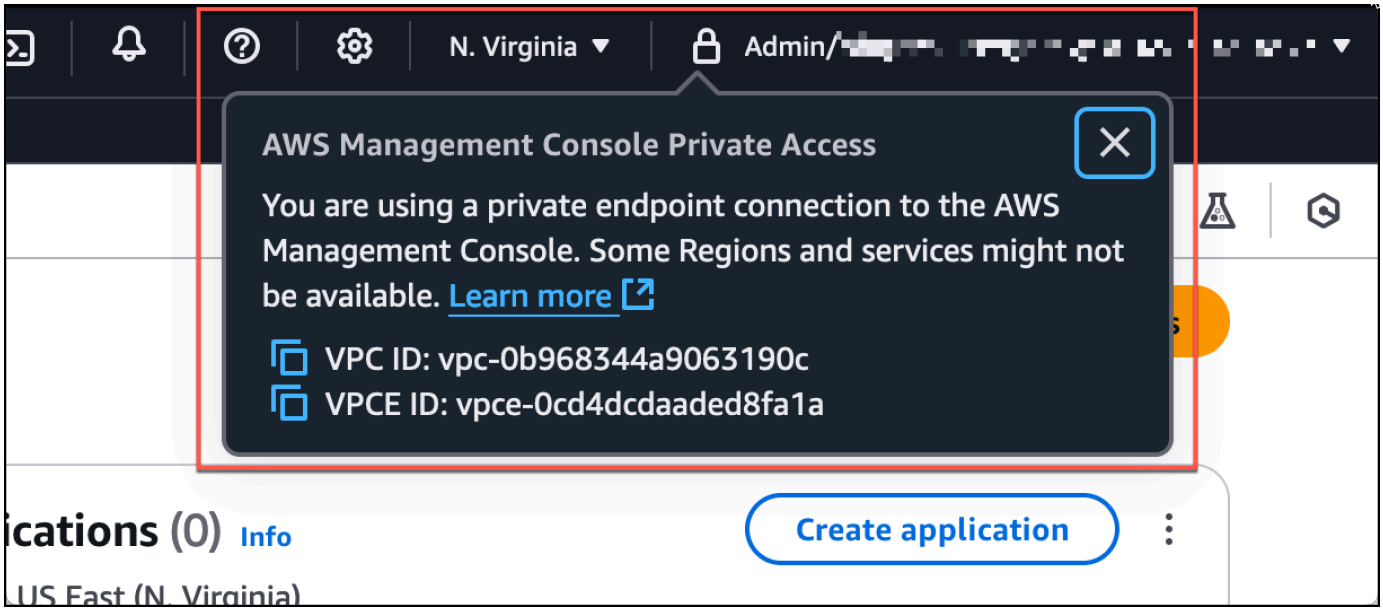
1. Masuk ke akun manajemen untuk organisasi Anda dan buka konsol Amazon EC2.
2. Di panel navigasi, pilih Instans.
3. Pada halaman Instans, pilih Instans pengujian VPCE konsol yang dibuat oleh template. CloudFormation Kemudian pilih Connect.

> **Note**
>
> Contoh ini menggunakan Fleet Manager, kemampuan AWS Systems Manager Explorer, untuk terhubung ke Windows Server Anda. Mungkin perlu beberapa menit sebelum koneksi dapat dimulai.

4. Pada halaman Connect to instance, pilih RDP Client, lalu Connect menggunakan Fleet Manager.
5. Pilih Desktop Jarak Jauh Manajer Armada.
6. Untuk mendapatkan kata sandi administratif untuk instans Amazon EC2 dan mengakses Desktop Windows menggunakan antarmuka web, gunakan kunci pribadi yang terkait dengan key pair Amazon EC2 yang Anda gunakan saat CloudFormation membuat template.
7. Dari instans Windows Amazon EC2, buka Konsol Manajemen AWS di browser.
8. Setelah Anda masuk dengan AWS kredensyal Anda, buka konsol Amazon S3 dan verifikasi bahwa Anda terhubung Konsol Manajemen AWS menggunakan Akses Pribadi.

Untuk menguji pengaturan Akses Konsol Manajemen AWS Pribadi

1. Masuk ke akun manajemen untuk organisasi Anda dan buka konsol Amazon S3.
2. Pilih ikon kunci-pribadi di bilah navigasi untuk melihat titik akhir VPC yang digunakan. Tangkapan layar berikut menunjukkan lokasi ikon kunci-pribadi dan informasi VPC.



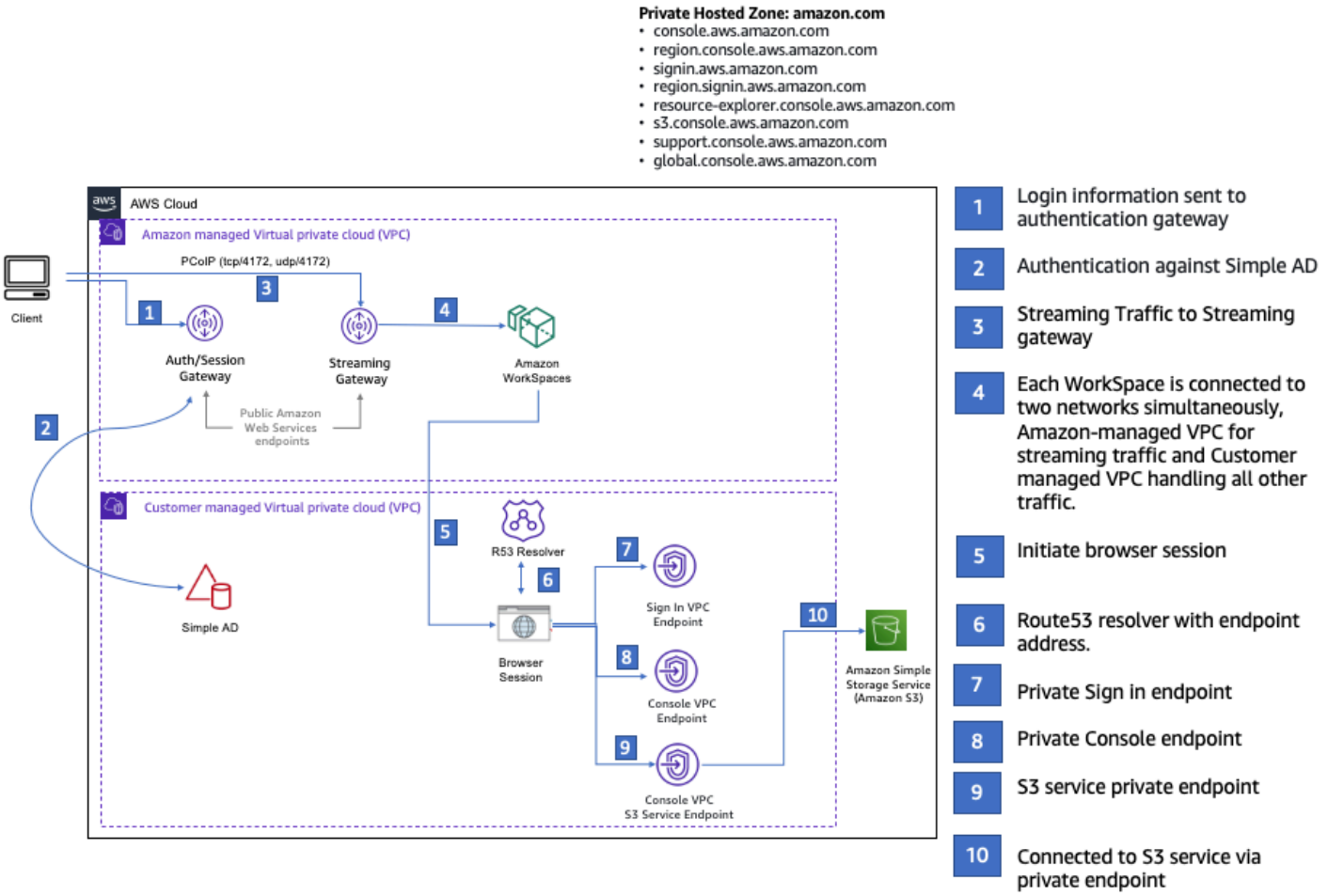

## Uji pengaturan dengan Amazon WorkSpaces

Amazon WorkSpaces memungkinkan Anda menyediakan desktop Windows, Amazon Linux, atau Ubuntu Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai. WorkSpaces Anda dapat dengan cepat menambahkan atau menghapus pengguna saat kebutuhan Anda berubah. Pengguna dapat mengakses desktop virtual mereka dari beberapa perangkat atau peramban web. Untuk mempelajari selengkapnya WorkSpaces, lihat Panduan WorkSpaces Administrasi Amazon.

Contoh di bagian ini menjelaskan lingkungan pengujian di mana lingkungan pengguna menggunakan browser web yang berjalan pada WorkSpace untuk masuk ke Akses Konsol Manajemen AWS Pribadi. Kemudian, pengguna mengunjungi konsol Amazon Simple Storage Service. Ini WorkSpace dimaksudkan untuk mensimulasikan pengalaman pengguna korporat dengan laptop pada jaringan yang terhubung dengan VPC, mengakses dari browser mereka. Konsol Manajemen AWS

Tutorial ini digunakan AWS CloudFormation untuk membuat dan mengkonfigurasi pengaturan jaringan dan Simple Active Directory untuk digunakan WorkSpaces bersama dengan petunjuk langkah demi langkah untuk setup WorkSpace menggunakan Konsol Manajemen AWS.

Diagram berikut menjelaskan alur kerja untuk menggunakan WorkSpace untuk menguji penyiapan Akses Konsol Manajemen AWS Pribadi. Ini menunjukkan hubungan antara klien WorkSpace, VPC yang dikelola Amazon, dan VPC yang dikelola pelanggan.




Salin CloudFormation template berikut dan simpan ke file yang akan Anda gunakan pada langkah 3 prosedur untuk mengatur jaringan.

Konsol Manajemen AWS CloudFormation Templat lingkungan Akses Pribadi

```
Description: |
  AWS Management Console Private Access.
Parameters:

  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
```

```
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  DSAdminPasswordResourceName:
    Type: String
    Default: ADAdminSecret
    Description: Password for directory services admin

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
```

```
      az2: apse1-az2
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - lambda.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
      Policies:
        - PolicyName: describe-ec2-az
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
```

```
              - Effect: Allow
                Action:
                  - 'ec2:DescribeAvailabilityZones'
                Resource: '*'
      MaxSessionDuration: 3600
      Path: /service-role/

  fnZoneIdtoZoneName:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.8
      Handler: index.lambda_handler
      Code:
        ZipFile: |
          import boto3
          import cfnresponse

          def zoneId_to_zoneName(event, context):
              responseData = {}
              ec2 = boto3.client('ec2')
              describe_az = ec2.describe_availability_zones()
              for az in describe_az['AvailabilityZones']:
                  if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                      responseData['ZoneName'] = az['ZoneName']
                      cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

          def no_op(event, context):
              print(event)
              responseData = {}
              cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

          def lambda_handler(event, context):
              if event['RequestType'] == ('Create' or 'Update'):
                  zoneId_to_zoneName(event, context)
              else:
                  no_op(event,context)
      Role: !GetAtt iamLambdaExecutionRole.Arn

  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
```

```
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

########################
# VPC AND SUBNETS
########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
```

```
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

########################
# Route Tables
########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
```

```
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
```

```
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC
```

```
#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
```

```
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  WidgetProxyRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref "ConsoleHostedZone"
      Name: "*.widget.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
        HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      Type: A

  ConsoleRecordRegional:
```

```
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegionalMultiSession:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
```

```
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# WORKSPACE RESOURCES
#########################
  ADAdminSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      Name: !Ref DSAdminPasswordResourceName
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: PrivateSubnetA
          - Ref: PrivateSubnetB

        VpcId:
          Ref: AppVPC
```

```
Outputs:
  PrivateSubnetA:
    Description: Private Subnet A
    Value: !Ref PrivateSubnetA

  PrivateSubnetB:
    Description: Private Subnet B
    Value: !Ref PrivateSubnetB

  WorkspaceSimpleDirectory:
    Description: Directory to be used for Workspaces
    Value: !Ref WorkspaceSimpleDirectory

  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
 Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

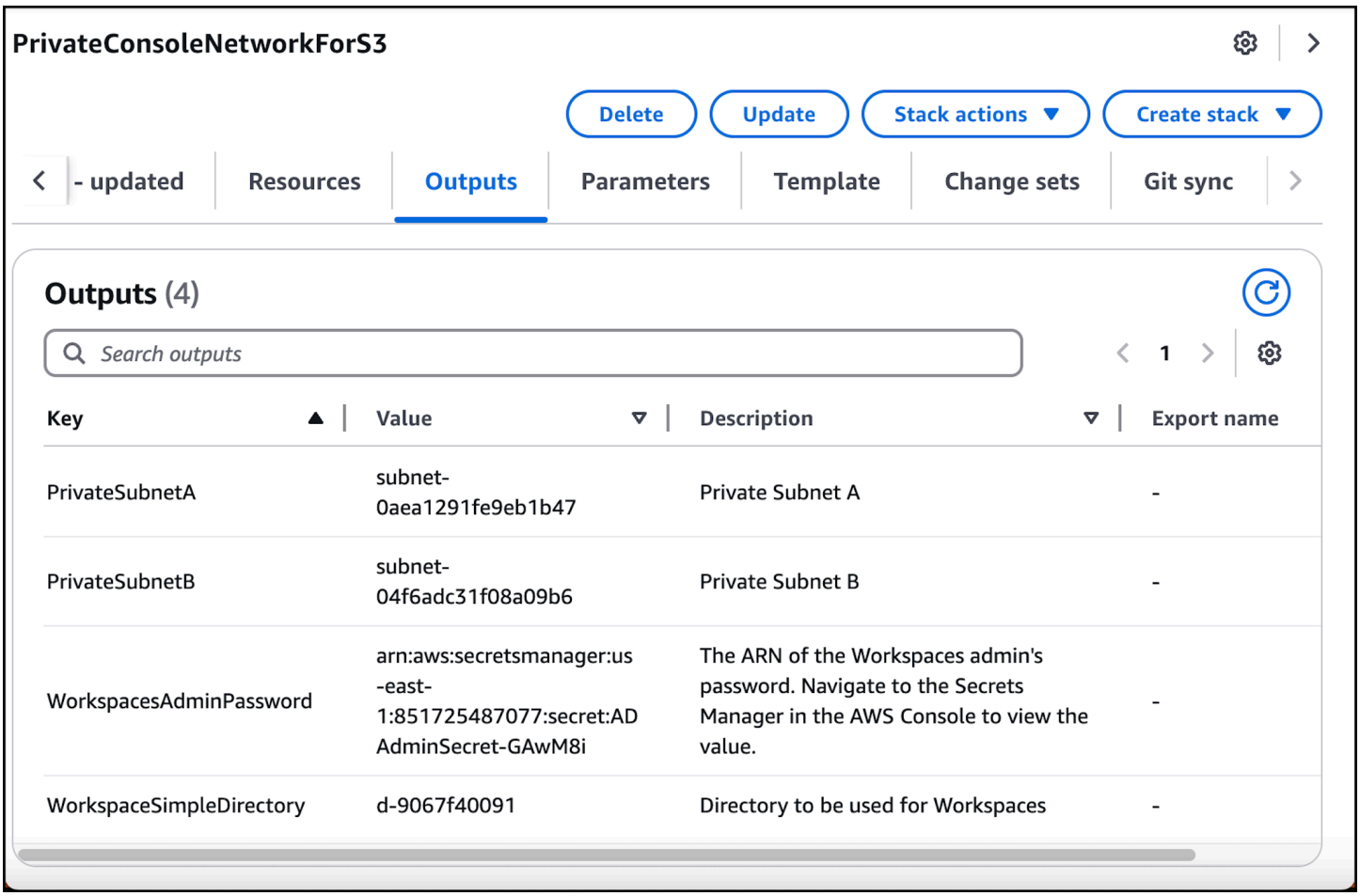
> **Note**
>
> Pengaturan pengujian ini dirancang untuk berjalan di Wilayah AS Timur (Virginia N.) (us-east-1).

Untuk mengatur jaringan

1. Masuk ke akun manajemen untuk organisasi Anda dan buka CloudFormation konsol.
2. Pilih Buat tumpukan.
3. Pilih Dengan sumber daya baru (standar). Unggah file CloudFormation template yang sebelumnya Anda buat, dan pilih Berikutnya.
4. Masukkan nama untuk tumpukan, seperti**`PrivateConsoleNetworkForS3`**, lalu pilih Berikutnya.
5. Untuk VPC dan subnet, masukkan rentang CIDR IP pilihan Anda, atau gunakan nilai default yang disediakan. Jika Anda menggunakan nilai default, verifikasi bahwa nilai tersebut tidak tumpang tindih dengan sumber daya VPC yang ada di Anda. Akun AWS
6. Pilih Buat tumpukan.
7. Setelah tumpukan dibuat, pilih tab Resources untuk melihat sumber daya yang telah dibuat.

8. Pilih tab Output, untuk melihat nilai untuk subnet pribadi dan Workspace Simple Directory. Catat nilai-nilai ini, karena Anda akan menggunakannya pada langkah keempat dari prosedur berikutnya untuk membuat dan mengonfigurasi file. WorkSpace

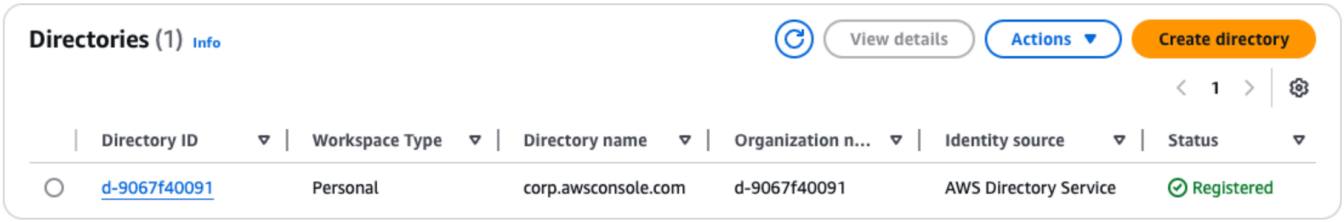
Tangkapan layar berikut menunjukkan tampilan tab Output yang menampilkan nilai untuk subnet pribadi dan Direktori Sederhana Ruang Kerja.




Sekarang setelah Anda membuat jaringan, gunakan prosedur berikut untuk membuat dan mengakses file WorkSpace.

Untuk membuat WorkSpace

1. Buka konsol WorkSpaces .
2. Di panel navigasi, pilih Direktori.
3. Pada halaman Direktori, verifikasi bahwa status direktori adalah Aktif. Screenshot berikut menunjukkan halaman Direktori dengan direktori aktif.




4. Untuk menggunakan direktori di WorkSpaces, Anda harus mendaftarkannya. Di panel navigasi, pilih WorkSpaces, lalu pilih Buat WorkSpaces.
5. Untuk Pilih direktori, pilih direktori yang dibuat oleh CloudFormation dalam prosedur sebelumnya. Pada menu Tindakan, pilih Daftar.
6. Untuk pemilihan subnet, pilih dua subnet pribadi yang dicatat pada langkah sembilan dari prosedur sebelumnya.
7. Pilih Aktifkan izin layanan mandiri, lalu pilih Daftar.
8. Setelah direktori terdaftar, lanjutkan membuat file WorkSpace. Pilih direktori yang terdaftar, lalu pilih Berikutnya.
9. Pada halaman Buat pengguna, pilih Buat pengguna tambahan. Masukkan nama dan email Anda untuk memungkinkan Anda menggunakan file WorkSpace. Verifikasi bahwa alamat email valid karena informasi WorkSpace login dikirim ke alamat email ini.
10. Pilih Berikutnya.
11. Pada halaman Identifikasi Pengguna, pilih pengguna yang Anda buat di langkah sembilan, lalu pilih Berikutnya.
12. Pada halaman Pilih Bundel, pilih Standar dengan Amazon Linux 2, lalu pilih Berikutnya.
13. Gunakan pengaturan default untuk mode berjalan dan kustomisasi pengguna, lalu pilih Buat Ruang Kerja. WorkSpace Dimulai dalam `Pending` status dan transisi ke `Available` dalam waktu sekitar 20 menit.
14. Ketika WorkSpace tersedia, Anda akan menerima email dengan instruksi untuk mengaksesnya di alamat email yang Anda berikan pada langkah sembilan.

Setelah Anda masuk WorkSpace, Anda dapat menguji apakah Anda mengaksesnya menggunakan Akses Konsol Manajemen AWS Pribadi Anda.

Untuk mengakses a WorkSpace

1. Buka email yang Anda terima di langkah 14 dari prosedur sebelumnya.

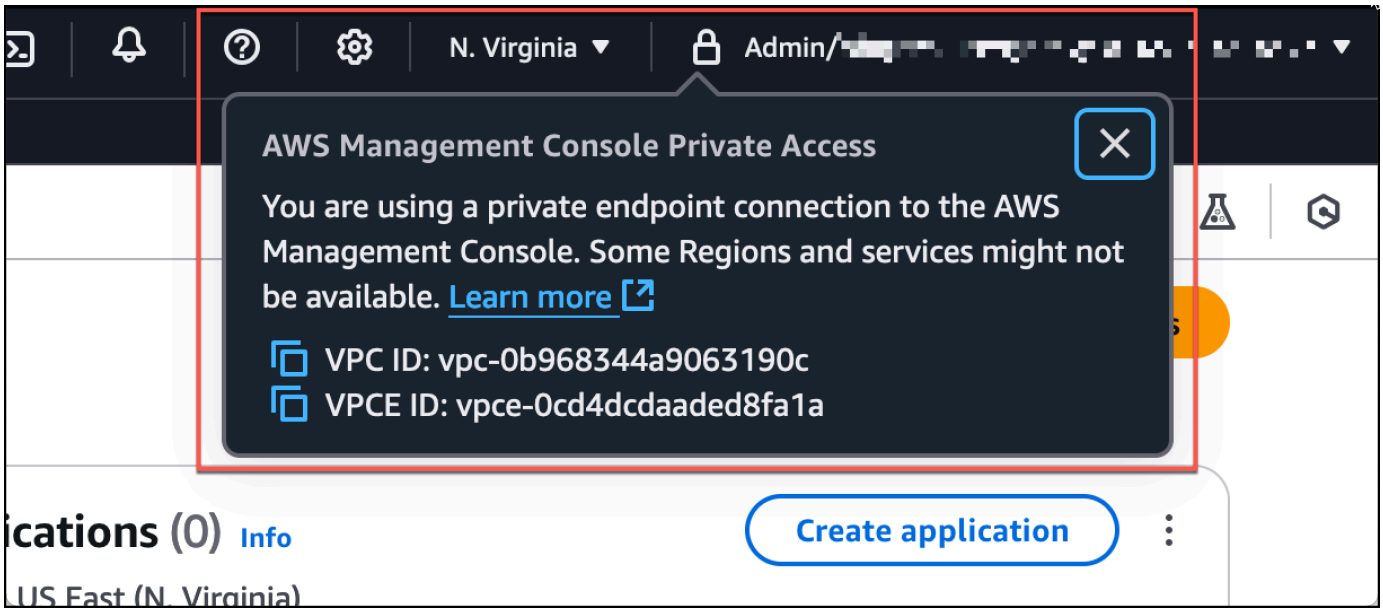
2. Di email, pilih tautan unik yang disediakan untuk mengatur profil Anda dan mengunduh WorkSpaces klien.
3. Atur kata sandi Anda.
4. Unduh klien pilihan Anda.
5. Instal dan luncurkan klien. Masukkan kode registrasi yang disediakan di email Anda, lalu pilih Daftar.
6. Masuk ke Amazon WorkSpaces menggunakan kredensi yang Anda buat di langkah ketiga.

Untuk menguji pengaturan Akses Konsol Manajemen AWS Pribadi

1. Dari Anda WorkSpace, buka browser Anda. Kemudian, navigasikan ke Konsol Manajemen AWSdan masuk menggunakan kredensional Anda.

> **Note**
>
> Jika Anda menggunakan Firefox sebagai browser Anda, verifikasi bahwa opsi Aktifkan DNS melalui HTTPS dimatikan di pengaturan browser Anda.

2. Buka konsol Amazon S3 tempat Anda dapat memverifikasi bahwa Anda terhubung menggunakan Akses Konsol Manajemen AWS Pribadi.
3. Pilih ikon kunci-pribadi pada bilah navigasi untuk melihat titik akhir VPC dan VPC yang digunakan. Tangkapan layar berikut menunjukkan lokasi ikon kunci-pribadi dan informasi VPC.



# Uji pengaturan VPC dengan kebijakan IAM

Anda dapat menguji lebih lanjut VPC yang telah Anda atur dengan Amazon EC2 WorkSpaces atau dengan menerapkan kebijakan IAM yang membatasi akses.

Kebijakan berikut menolak akses ke Amazon S3 kecuali menggunakan VPC yang Anda tentukan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "vpc-12345678"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
            }
        }
    ]
}
```

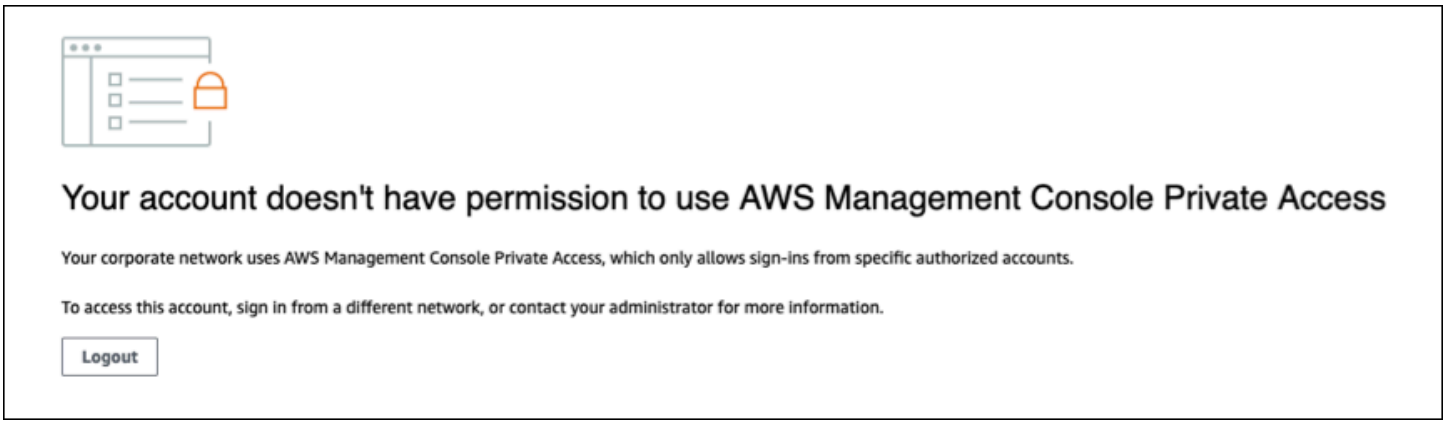
Kebijakan berikut membatasi login untuk dipilih Akun AWS IDs menggunakan kebijakan Akses Konsol Manajemen AWS Pribadi untuk titik akhir masuk.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
    ]
}
```

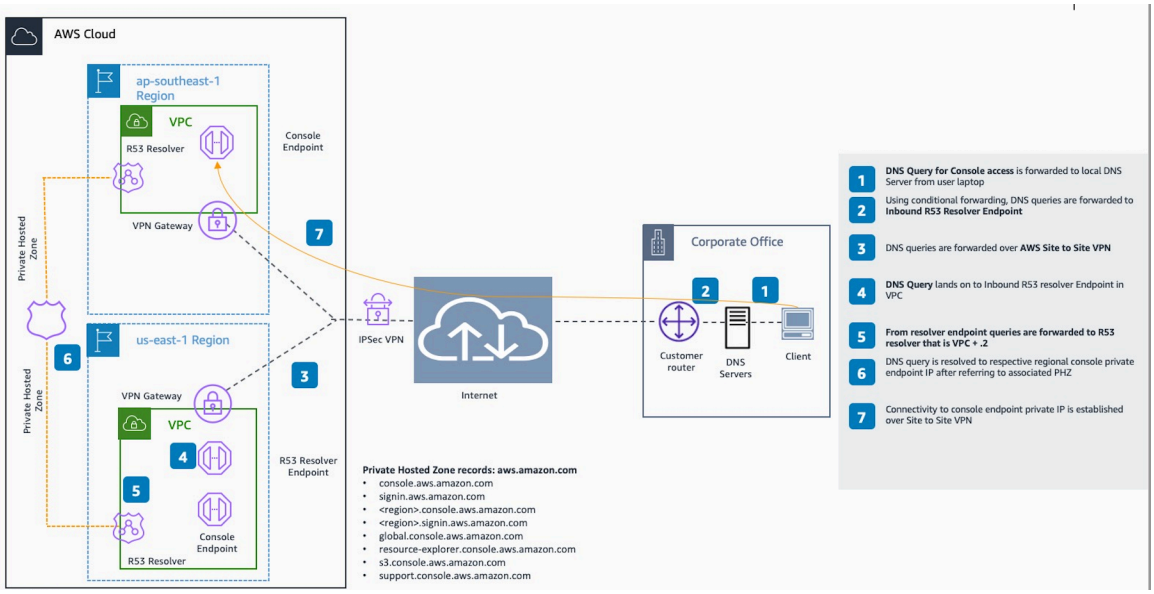
Jika Anda terhubung dengan identitas yang bukan milik akun Anda, halaman kesalahan berikut akan ditampilkan.




# Arsitektur referensi

Untuk terhubung secara pribadi ke Akses Konsol Manajemen AWS Pribadi dari jaringan lokal, Anda dapat memanfaatkan opsi koneksi AWS Site-to-Site VPN ke AWS Virtual Private Gateway (VGW). AWS Site-to-Site VPN memungkinkan akses ke jaringan jarak jauh Anda dari VPC Anda dengan membuat koneksi, dan mengonfigurasi perutean untuk melewati lalu lintas melalui koneksi. Untuk informasi selengkapnya, lihat Apa itu AWS VPN Site-to-Site di Panduan Pengguna VPN.AWS Site-to-Site  AWS Virtual Private Gateway (VGW) adalah layanan Regional yang sangat tersedia yang bertindak sebagai gateway antara VPC dan jaringan lokal.

AWS Site-to-Site VPN ke Gerbang Pribadi AWS Virtual (VGW)




Komponen penting dalam desain arsitektur referensi ini adalah Amazon Route 53 Resolver, khususnya inbound resolver. Saat Anda mengaturnya di VPC tempat titik akhir Akses Konsol Manajemen AWS Pribadi dibuat, titik akhir resolver (antarmuka jaringan) dibuat di subnet yang ditentukan. Alamat IP mereka kemudian dapat dirujuk dalam penerusan bersyarat di DNS server lokal, untuk memungkinkan kueri catatan di Zona Hosting Pribadi. Ketika klien lokal terhubung ke Konsol Manajemen AWS, mereka dirutekan ke titik akhir Konsol Manajemen AWS Private Access pribadi. IPs

Sebelum menyiapkan koneksi ke titik akhir Akses Konsol Manajemen AWS Pribadi, selesaikan langkah-langkah prasyarat untuk menyiapkan titik akhir Akses Konsol Manajemen AWS Pribadi di semua Wilayah tempat Anda ingin mengakses Konsol Manajemen AWS, serta di Wilayah AS Timur (Virginia N.), dan mengonfigurasi Zona Dihosting Pribadi.

# AWS Kustomisasi Pengalaman Pengguna (UXC)

AWS User Experience Customization (UXC) adalah utilitas yang memungkinkan administrator akun menyesuaikan tampilan visual Konsol Manajemen AWS dan mengelola pengaturan ini di tingkat akun.

Dengan UXC, Anda dapat menyesuaikan pengaturan berikut:

- Warna akun — Anda dapat mengatur warna untuk akun Anda untuk membedakannya secara visual. Misalnya, Anda dapat menggunakan hijau untuk akun pengembangan, kuning untuk akun pengujian, dan merah untuk akun produksi.
- Visibilitas layanan — Anda dapat mengontrol AWS layanan mana yang muncul di navigasi konsol. Visibilitas layanan menyederhanakan Konsol Manajemen AWS untuk hanya menampilkan AWS layanan yang relevan dengan akun Anda.
- Visibilitas wilayah - Anda dapat mengontrol AWS Wilayah mana yang muncul di pemilih Wilayah. Visibilitas wilayah menyederhanakan Konsol Manajemen AWS untuk hanya menampilkan Wilayah yang relevan dengan akun Anda.

Jika Anda belum mengonfigurasi setelan, maka perilaku default berlaku: semua layanan dan Wilayah terlihat, dan tidak ada warna akun yang disetel. Anda dapat mengatur ulang warna akun ke defaultnya dengan menyetel nilainya`"none"`. Anda dapat mengatur ulang layanan dan Wilayah yang terlihat ke defaultnya dengan menyetel nilainya. `null`

> **Note**
>
> `visibleRegions`Pengaturan `visibleServices` dan hanya mengontrol tampilan layanan dan Wilayah di Konsol Manajemen AWS. Mereka tidak membatasi akses melalui AWS Command Line Interface, SDKs, atau lainnya APIs.

Topik

- Memulai Kustomisasi Pengalaman AWS Pengguna
- Pencatatan panggilan API Kustomisasi Pengalaman AWS Pengguna menggunakan AWS CloudTrail
- Keamanan dalam Kustomisasi Pengalaman AWS Pengguna

# Memulai Kustomisasi Pengalaman AWS Pengguna

Dengan UXC, administrator akun dapat mengonfigurasi kustomisasi akun untuk file. Konsol Manajemen AWS

## Prasyarat

Sebelum memulai, Anda perlu melakukan hal berikut:

- Sebuah AWS akun
- Izin yang sesuai AWS Identity and Access Management (IAM) untuk UXC. Untuk informasi selengkapnya, lihat Cara Kustomisasi Pengalaman AWS Pengguna bekerja dengan IAM dan kebijakan AWS terkelola untuk. Konsol Manajemen AWS

## Mengakses pengaturan UXC di Konsol Manajemen AWS

Untuk mengakses warna akun di Konsol Manajemen AWS, lihat Mengakses informasi akun di. Konsol Manajemen AWS Untuk mengakses visibilitas layanan dan visibilitas Wilayah di bagian Konsol Manajemen AWS, lihat Mengonfigurasi Konsol Manajemen AWS menggunakan Setelan Terpadu.

Untuk mengatur warna akun di konsol

1. Masuk ke Konsol Manajemen AWS.
2. Di bilah navigasi, pilih nama akun Anda.
3. Pilih Akun.
4. Di Pengaturan tampilan akun, pilih warna.
5. Pilih Perbarui.

Untuk menyetel Wilayah yang terlihat di konsol

1. Masuk ke Konsol Manajemen AWS.
2. Buka Pengaturan Terpadu.
3. Pilih Edit di bagian Wilayah Terlihat.
4. Setel Wilayah yang terlihat ke Semua Wilayah yang tersedia atau Pilih Wilayah dan konfigurasikan daftar Anda.

5. Pilih Simpan perubahan.

Untuk mengatur layanan yang terlihat di konsol

1. Masuk ke Konsol Manajemen AWS.
2. Buka Pengaturan Terpadu.
3. Pilih Edit di bagian Layanan yang terlihat.
4. Setel layanan yang terlihat ke Semua layanan atau Pilih layanan dan konfigurasikan daftar Anda.
5. Pilih Simpan perubahan.

## Mengakses pengaturan UXC secara terprogram

Anda juga dapat mengelola pengaturan kustomisasi akun secara terprogram atau sebagai infrastruktur sebagai kode. Untuk informasi selengkapnya, lihat Referensi API Kustomisasi Pengalaman AWS Pengguna dan referensi AWS::UXC::AccountCustomization CloudFormation templat.

# Pencatatan panggilan API Kustomisasi Pengalaman AWS Pengguna menggunakan AWS CloudTrail

AWS Kustomisasi Pengalaman Pengguna terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. CloudTrail menangkap semua panggilan API untuk UXC sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol UXC dan panggilan kode ke operasi UXC API. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke UXC, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

## Acara manajemen UXC di CloudTrail

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. Ini juga dikenal sebagai operasi bidang kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

AWS Kustomisasi Pengalaman Pengguna mencatat semua operasi bidang kontrol UXC sebagai peristiwa manajemen. Untuk daftar operasi bidang kontrol Kustomisasi Pengalaman AWS Pengguna yang dicatat oleh UXC CloudTrail, lihat Referensi API Kustomisasi Pengalaman AWS Pengguna.

## Contoh acara UXC

Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang operasi API yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan CloudTrail peristiwa yang menunjukkan operasi.


```
{
  "eventVersion" : "1.09",
  "userIdentity" : {
    "type" : "AssumedRole",
    "principalId" : "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn" : "arn:aws:sts::111122223333:assumed-role/user/jdoe",
    "accountId" : "111122223333",
    "accessKeyId" : "AKIAIOSFODNN7EXAMPLE",
    "sessionContext" : {
      "sessionIssuer" : {
        "type" : "Role",
        "principalId" : "AIDACKCEVSQ6C2EXAMPLE",
        "arn" : "arn:aws:iam::111122223333:role/user",
        "accountId" : "111122223333",
        "userName" : "jdoe"
      },
      "webIdFederationData" : { },
      "attributes" : {
        "creationDate" : "2022-12-09T23:48:51Z",
        "mfaAuthenticated" : "false"
      }
    }
```

```
  },
  "eventTime" : "2022-12-09T23:50:03Z",
  "eventSource" : "uxc.amazonaws.com",
  "eventName" : "GetAccountColor",
  "awsRegion" : "us-east-2",
  "sourceIPAddress" : "10.24.34.3",
  "userAgent" : "PostmanRuntime/7.43.4",
  "requestParameters" : null,
  "responseElements" : null,
  "requestID" : "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
  "eventID" : "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
  "readOnly" : true,
  "eventType" : "AwsApiCall",
  "managementEvent" : true,
  "recipientAccountId" : "111122223333",
  "eventCategory" : "Management"
}
```


Untuk informasi tentang konten CloudTrail rekaman, lihat konten CloudTrail rekaman di Panduan AWS CloudTrail Pengguna.

## Keamanan dalam Kustomisasi Pengalaman AWS Pengguna

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Kustomisasi Pengalaman AWS Pengguna, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan UXC. Topik berikut menunjukkan cara mengonfigurasi UXC untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya UXC Anda.

Topik


- Identity and Access Management untuk Kustomisasi Pengalaman AWS Pengguna


# Identity and Access Management untuk Kustomisasi Pengalaman AWS Pengguna

AWS User Experience Customization (UXC) menggunakan kebijakan IAM untuk mengelola akses ke Operasi API UXC.

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Kustomisasi Pengalaman Pengguna. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik


- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Cara Kustomisasi Pengalaman AWS Pengguna bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk AWS Kustomisasi Pengalaman Pengguna


## Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Pemecahan Masalah Pengalaman AWS Pengguna Identitas dan akses kustomisasi)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Cara Kustomisasi Pengalaman AWS Pengguna bekerja dengan IAM)

- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Contoh kebijakan berbasis identitas untuk AWS Kustomisasi Pengalaman Pengguna)

## Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensional dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau kredensional. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

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

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

### Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

## Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

### Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

### Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

### Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — Tentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

### Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

## Cara Kustomisasi Pengalaman AWS Pengguna bekerja dengan IAM

AWS User Experience Customization (UXC) bekerja dengan kebijakan IAM untuk mengelola akses ke Operasi API UXC.

Sebelum Anda menggunakan IAM untuk mengelola akses ke Kustomisasi Pengalaman AWS Pengguna (Kustomisasi Pengalaman Pengguna), pelajari fitur IAM apa yang tersedia untuk digunakan dengan Kustomisasi Pengalaman Pengguna. Kami menyarankan Anda mengintegrasikan dengan Kustomisasi Pengalaman Pengguna melalui kebijakan AWS terkelola, untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk Konsol Manajemen AWS.

Sebelum Anda menggunakan IAM untuk mengelola akses ke Kustomisasi Pengalaman Pengguna, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Kustomisasi Pengalaman Pengguna.

| Fitur IAM | Dukungan Kustomisasi Pengalaman Pengguna |
|---|---|
| Kebijakan berbasis identitas | Ya |
| Kebijakan berbasis sumber daya | Tidak |
| Tindakan kebijakan | Ya |
| Sumber daya kebijakan | Tidak |
| Kunci kondisi kebijakan | Tidak |
| Kredensial sementara | Ya |
| Izin utama lintas layanan | Tidak |
| Peran terkait layanan | Tidak |
| Peran layanan | Tidak |

Untuk mendapatkan tampilan tingkat tinggi tentang cara Kustomisasi Pengalaman Pengguna dan AWS layanan lainnya bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Kustomisasi Pengalaman Pengguna

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas,

lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Untuk melihat contoh kebijakan berbasis identitas Kustomisasi Pengalaman Pengguna, lihat Contoh kebijakan berbasis identitas untuk Kustomisasi Pengalaman Pengguna. AWS

Tindakan kebijakan untuk Kustomisasi Pengalaman Pengguna

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat semua tindakan Kustomisasi Pengalaman Pengguna, lihat Referensi API.

Tindakan kebijakan dalam Kustomisasi Pengalaman Pengguna menggunakan `uxc:` awalan sebelum tindakan (misalnya`uxc:GetAccountCustomizations`).

Untuk menentukan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma:

```
"Action": [
      "uxc:GetAccountCustomizations",
      "uxc:ListServices"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Kustomisasi Pengalaman Pengguna, lihat Contoh kebijakan berbasis identitas untuk Kustomisasi Pengalaman Pengguna. AWS

Sumber daya kebijakan untuk Kustomisasi Pengalaman Pengguna

Kustomisasi Pengalaman Pengguna tidak mendukung sumber daya kebijakan.

Menggunakan kredensil sementara dengan Kustomisasi Pengalaman Pengguna

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Pemecahan Masalah Pengalaman AWS Pengguna Identitas dan akses kustomisasi

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Kustomisasi Pengalaman Pengguna dan IAM.

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `uxc:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 uxc:GetWidget on resource: my-example-widget because no identity-based policy allows
 the GetWidget action
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `uxc:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Setelah membuat access key pengguna IAM, Anda dapat melihat access key ID Anda setiap saat. Namun, Anda tidak dapat melihat secret access key Anda lagi. Jika Anda kehilangan secret key, Anda harus membuat pasangan access key baru.

Access key terdiri dari dua bagian: access key ID (misalnya, `AKIAIOSFODNN7EXAMPLE`) dan secret access key (misalnya, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Seperti nama pengguna dan kata sandi, Anda harus menggunakan access key ID dan secret access key sekaligus untuk mengautentikasi permintaan Anda. Kelola access key Anda seaman nama pengguna dan kata sandi Anda.

> **Important**
>
> Jangan memberikan access key Anda kepada pihak ke tiga, bahkan untuk membantu menemukan ID pengguna kanonis Anda. Dengan melakukan ini, Anda mungkin memberi seseorang akses permanen ke Anda Akun AWS.

Saat Anda membuat pasangan access key, Anda diminta menyimpan access key ID dan secret access key di lokasi yang aman. secret access key hanya tersedia saat Anda membuatnya. Jika Anda kehilangan secret access key Anda, Anda harus menambahkan access key baru ke pengguna IAM Anda. Anda dapat memiliki maksimum dua access key. Jika Anda sudah memiliki dua, Anda harus menghapus satu pasangan kunci sebelum membuat pasangan baru. Untuk melihat instruksi, lihat Mengelola access keys di Panduan Pengguna IAM.

Untuk memungkinkan orang lain mengakses Kustomisasi Pengalaman Pengguna, Anda harus memberikan izin kepada orang atau aplikasi yang membutuhkan akses. Jika Anda menggunakan AWS IAM Identity Center untuk mengelola orang dan aplikasi, Anda menetapkan set izin kepada pengguna atau grup untuk menentukan tingkat akses mereka. Set izin secara otomatis membuat dan menetapkan kebijakan IAM ke peran IAM yang terkait dengan orang atau aplikasi. Untuk informasi selengkapnya, lihat Set izin di Panduan AWS IAM Identity Center Pengguna.

Jika Anda tidak menggunakan IAM Identity Center, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Anda kemudian harus melampirkan kebijakan ke entitas yang memberi mereka izin yang benar dalam Kustomisasi Pengalaman Pengguna. Setelah izin diberikan, berikan kredensialnya kepada pengguna atau pengembang aplikasi. Mereka akan menggunakan kredensil tersebut untuk mengakses. AWSUntuk mempelajari selengkapnya tentang membuat pengguna, grup, kebijakan, dan izin IAM, lihat Identitas dan Kebijakan IAM dan izin di IAM di Panduan Pengguna IAM.

## Contoh kebijakan berbasis identitas untuk AWS Kustomisasi Pengalaman Pengguna

Secara default, pengguna dan peran tidak memiliki izin untuk mendapatkan atau memodifikasi sumber daya UXC. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya, administrator IAM dapat membuat kebijakan IAM. Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Akses hanya-baca ke Kustomisasi Akun UXC
- Akses penuh ke Kustomisasi Akun UXC

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Kustomisasi Pengalaman Pengguna di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk

informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.

- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Akses hanya-baca ke Kustomisasi Akun UXC

Contoh berikut menunjukkan cara membuat kebijakan yang memungkinkan akses hanya-baca ke Penyesuaian Akun UXC:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "uxc:GetAccountCustomizations",
                "uxc:ListServices"
            ],
            "Resource": "*"
        }
    ]
}
```

Akses penuh ke Kustomisasi Akun UXC

Contoh berikut menunjukkan cara membuat kebijakan yang memungkinkan akses penuh ke Kustomisasi Akun UXC:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "uxc:*"
            ],
            "Resource": "*"
        }
    ]
}
```

# AWS kebijakan terkelola untuk Konsol Manajemen AWS

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

# AWS kebijakan terkelola: AWSManagement ConsoleBasicUserAccess

Anda dapat melampirkan `AWSManagementConsoleBasicUserAccess` ke pengguna, grup, dan peran Anda.

Kebijakan ini memberikan izin yang diperlukan untuk pengguna non-administratif. Konsol Manajemen AWS Ini termasuk fitur seperti penemuan sumber daya, notifikasi, akses shell berbasis browser, dan navigasi yang disesuaikan.

Detail izin

`AWSManagementConsoleBasicUserAccess`Ini dikelompokkan ke dalam kumpulan izin berikut:

- `cloudshell`— Memungkinkan kepala sekolah akses penuh ke AWS CloudShell kemampuan, termasuk pembuatan lingkungan, manajemen sesi, dan eksekusi perintah.
- `ec2`— Memungkinkan kepala sekolah untuk menggambarkan Wilayah yang diaktifkan untuk akun di Navigasi Terpadu.
- `notifications`— Memungkinkan kepala sekolah untuk mendapatkan acara dari. Notifikasi Pengguna AWS
- `q`— Memungkinkan kepala sekolah untuk mengobrol dengan Pengembang Amazon Q.
- `resource-explorer-2`— Memungkinkan kepala sekolah untuk mencari dan menemukan AWS sumber daya menggunakan Pencarian Terpadu.
- `uxc`— Memungkinkan kepala sekolah membaca pengaturan Kustomisasi Pengalaman AWS Pengguna.
- `action-recommendations`— Memungkinkan kepala sekolah untuk menerima rekomendasi tindakan kontekstual.
- `account`— Memungkinkan kepala sekolah untuk mengambil informasi tentang akun yang ditentukan termasuk nama akun, ID akun, dan tanggal dan waktu pembuatan akun.

Untuk melihat izin kebijakan ini, lihat AWSManagementConsoleBasicUserAccessdi Referensi Kebijakan AWS Terkelola.

## AWS kebijakan terkelola: AWSManagement ConsoleAdministratorAccess

Anda dapat melampirkan `AWSManagementConsoleAdministratorAccess` ke pengguna, grup, dan peran Anda.

Kebijakan ini memberikan akses penuh untuk mengonfigurasi dan menyesuaikan. Konsol Manajemen AWS Hal ini memungkinkan administrator untuk mengatur warna akun, mengaktifkan pemberitahuan pengguna, dan mengkonfigurasi penemuan sumber daya. Ini juga mencakup izin dari kebijakan `AWSManagementConsoleBasicUserAccess` terkelola, yang penting bagi pengguna non-administratif. Konsol Manajemen AWS

Detail izin

`AWSManagementConsoleAdministratorAccess`Ini dikelompokkan ke dalam kumpulan izin berikut:

- `cloudshell`— Memungkinkan kepala sekolah akses penuh ke AWS CloudShell kemampuan, termasuk pembuatan lingkungan, manajemen sesi, dan eksekusi perintah.
- `ec2`— Memungkinkan kepala sekolah untuk menggambarkan Wilayah yang diaktifkan untuk akun di Navigasi Terpadu.
- `notifications`— Memungkinkan kepala sekolah untuk mengakses dan memperbarui konfigurasi pemberitahuan, acara, dan status keikutsertaan fitur.
- `q`— Memungkinkan kepala sekolah untuk mengobrol dengan Pengembang Amazon Q untuk dukungan yang dibantu AI.
- `resource-explorer-2`— Memungkinkan kepala sekolah untuk mencari dan menemukan AWS sumber daya menggunakan Pencarian Terpadu.
- `uxc`— Memungkinkan kepala sekolah akses penuh ke pengaturan Kustomisasi Pengalaman AWS Pengguna.
- `action-recommendations`— Memungkinkan kepala sekolah untuk menerima rekomendasi tindakan kontekstual.
- `account`— Memungkinkan kepala sekolah untuk mengambil informasi tentang akun yang ditentukan termasuk nama akun, ID akun, dan tanggal dan waktu pembuatan akun.

Untuk melihat izin kebijakan ini, lihat AWSManagementConsoleAdministratorAccessdi Referensi Kebijakan AWS Terkelola.

## Konsol Manajemen AWS pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola Konsol Manajemen AWS sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat Konsol Manajemen AWS dokumen.

| Ubah | Deskripsi | Date |
| --- | --- | --- |
| AWSManagementConsoleBasicUserAccess— Kebijakan yang diperbarui | Ditambahkan `uxc:GetAccountCustomizations` dan `uxc:ListServices` izin. | Maret 26, 2026 |
| AWSManagementConsoleAdministratorAccess— Kebijakan yang diperbarui | Ditambahkan`uxc:GetAccountCustomizations` ,`uxc:UpdateAccountCustomizations` , dan `uxc:ListServices` izin. | Maret 26, 2026 |
| AWSManagementConsoleBasicUserAccess— Kebijakan yang diperbarui | Kebijakan yang diperbarui untuk menambahkan izin agar pengguna dapat melihat informasi akun dan menerima rekomendasi tindakan saat menavigasi. Konsol Manajemen AWS | Desember 9, 2025 |
| AWSManagementConsoleAdministratorAccess— Kebijakan yang diperbarui | Kebijakan yang diperbarui untuk menambahkan izin agar pengguna dapat melihat informasi akun dan menerima rekomendasi tindakan saat menavigasi. Konsol Manajemen AWS | Desember 9, 2025 |
| AWSManagementConsoleBasicUserAccess – Kebijakan baru | Menambahkan kebijakan AWS terkelola baru yang memberikan izin yang diperlukan untuk Konsol Manajemen AWS navigasi dasar, tampilan warna akun, dan penemuan sumber daya. | Agustus 14, 2025 |

| Ubah | Deskripsi | Date |
| --- | --- | --- |
| AWSManagementConsoleAdministratorAccess – Kebijakan baru | Menambahkan kebijakan AWS terkelola baru yang menyediakan akses penuh untuk mengonfigurasi dan menyesuaikan Konsol Manajemen AWS. | Agustus 14, 2025 |
| Konsol Manajemen AWS mulai melacak perubahan | Konsol Manajemen AWS mulai melacak perubahan untuk kebijakan AWS terkelola nya. | Agustus 14, 2025 |

# Menggunakan Markdown di Konsol

Beberapa layanan di Konsol Manajemen AWS, seperti Amazon CloudWatch, mendukung penggunaan Markdown di bidang tertentu. Topik ini menjelaskan jenis format Markdown yang didukung di konsol.

Daftar Isi


- Paragraf, Spasi Baris, dan Garis Horizontal
- Judul
- Format Teks
- Tautan
- Daftar
- Tabel dan Tombol (CloudWatch Dasbor)


## Paragraf, Spasi Baris, dan Garis Horizontal

Paragraf dipisahkan oleh baris kosong. Untuk memastikan bahwa baris kosong antara paragraf ditampilkan ketika dikonversi ke HTML, tambahkan baris baru dengan non-break space (` `) dan kemudian baris kosong. Ulangi pasangan baris ini untuk menyisipkan beberapa baris kosong satu demi satu, seperti pada contoh berikut:

```
 

 
```

Untuk membuat aturan horizontal yang memisahkan paragraf, tambahkan baris baru dengan tiga tanda hubung berturut-turut: `---`

```
Previous paragraph.
---
Next paragraph.
```

Untuk membuat blok teks dengan tipe monospace, tambahkan baris dengan tiga backticks (). ` Masukkan teks untuk ditampilkan dalam tipe monospace. Kemudian, tambahkan baris baru lainnya

dengan tiga backticks. Contoh berikut menunjukkan teks yang akan diformat ke tipe monospace saat ditampilkan:

```
```
This appears in a text box with a background shading.
The text is in monospace.
```
```

## Judul

Untuk membuat judul, gunakan tanda pound (#). Tanda pound tunggal dan spasi menunjukkan heading tingkat atas. Dua tanda pound menciptakan heading level kedua, dan tiga tanda pound menciptakan heading tingkat ketiga. Contoh berikut menunjukkan judul tingkat atas, tingkat kedua, dan tingkat ketiga:

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

## Format Teks

Untuk memformat teks sebagai miring, mengelilinginya dengan satu garis bawah ( _ ) atau tanda bintang (*) di setiap sisi.

```
*This text appears in italics.*
```

Untuk memformat teks agar tercetak tebal, apit dengan dua garis bawah atau dua tanda bintang di setiap sisi.

```
**This text appears in bold.**
```

Untuk memformat teks sebagai coretan, kelilingi dengan dua tildes (~) di setiap sisi.

```
~~This text appears in strikethrough.~~
```

# Tautan

Untuk menambahkan hyperlink teks, masukkan teks tautan yang dikelilingi oleh tanda kurung siku ([]), diikuti dengan URL lengkap dalam tanda kurung (()), seperti pada contoh berikut:

```
Choose [link_text](http://my.example.com).
```

# Daftar

Untuk memformat baris sebagai bagian dari daftar berpoin, tambahkan pada baris terpisah yang dimulai dengan tanda bintang tunggal (*) dan kemudian spasi, seperti pada contoh berikut:

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

Untuk memformat baris sebagai bagian dari daftar bernomor, tambahkan pada baris terpisah yang dimulai dengan angka, periode (.), dan spasi, seperti pada contoh berikut:

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

# Tabel dan Tombol (CloudWatch Dasbor)

CloudWatch widget teks dasbor mendukung tabel dan tombol Markdown.

Untuk membuat tabel, pisahkan kolom menggunakan bilah vertikal (|) dan baris menggunakan baris baru. Untuk membuat baris pertama sebagai baris header, masukkan garis antara baris header dan baris pertama nilai. Kemudian, tambahkan setidaknya tiga tanda hubung (-) untuk setiap kolom dalam tabel. Pisahkan kolom menggunakan bilah vertikal. Contoh berikut menunjukkan Markdown untuk tabel dengan dua kolom, baris header, dan dua baris data:

```
Table | Header
----|-----
Amazon Web Services | AWS
```

```
1 | 2
```

Teks Markdown pada contoh sebelumnya membuat tabel berikut:

| Tabel | Header |
| --- | --- |
| Amazon Web Services | AWS |
| 1 | 2 |

Di widget teks CloudWatch dasbor, Anda juga dapat memformat hyperlink agar muncul sebagai tombol. Untuk membuat tombol, gunakan`[button:`*`Button text`*`]`, diikuti dengan URL lengkap dalam tanda kurung (()), seperti pada contoh berikut:

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

# Pemecahan Masalah

Konsultasikan bagian ini untuk menemukan solusi untuk masalah umum dengan Konsol Manajemen AWS.

Anda juga dapat mendiagnosis dan memecahkan masalah kesalahan umum untuk beberapa AWS layanan menggunakan Amazon Q Developer. Untuk informasi selengkapnya, lihat Mendiagnosis kesalahan umum di konsol dengan Pengembang Amazon Q di Panduan Pengguna Pengembang Amazon Q.

Topik


- Halaman tidak dimuat dengan benar
- Browser saya menampilkan kesalahan 'akses ditolak' saat menghubungkan ke Konsol Manajemen AWS
- Browser saya menampilkan kesalahan batas waktu saat menghubungkan ke Konsol Manajemen AWS
- Saya ingin mengubah bahasa Konsol Manajemen AWS tetapi saya tidak dapat menemukan menu pemilihan bahasa di bagian bawah halaman


## Halaman tidak dimuat dengan benar

- Jika masalah ini hanya terjadi sesekali, periksa koneksi internet Anda. Cobalah untuk terhubung melalui jaringan yang berbeda, atau dengan atau tanpa VPN, atau coba gunakan browser web yang berbeda.
- Jika semua pengguna yang terkena dampak berasal dari tim yang sama, itu mungkin ekstensi browser privasi atau masalah firewall keamanan. Ekstensi browser privasi dan firewall keamanan dapat memblokir akses ke domain yang digunakan oleh. Konsol Manajemen AWS Coba matikan ekstensi ini atau sesuaikan pengaturan firewall. Untuk memverifikasi masalah dengan koneksi Anda, buka alat pengembang browser Anda (Chrome, Firefox) dan periksa kesalahan di tab Konsol. Sufiks Konsol Manajemen AWS menggunakan domain termasuk daftar berikut. Daftar ini tidak lengkap dan dapat berubah seiring waktu. Sufiks domain ini tidak digunakan secara eksklusif oleh. AWS
  - .a2z.com
  - .amazon.com
  - .amazonaws.com

- .aws
- .aws.com
- .aws.dev
- .awscloud.com
- .awsplayer.com
- .awsstatic.com
- .cloudfront.net
- .live-video.net

> **Warning**
>
> Sejak 31 Juli 2022, AWS tidak lagi mendukung Internet Explorer 11. Kami menyarankan Anda menggunakan Konsol Manajemen AWS dengan browser lain yang didukung. Untuk informasi lebih lanjut, lihat Blog AWS Berita.

## Browser saya menampilkan kesalahan 'akses ditolak' saat menghubungkan ke Konsol Manajemen AWS

Perubahan terbaru yang dilakukan pada konsol dapat memengaruhi akses Anda jika semua kondisi berikut terpenuhi:

- Anda mengakses Konsol Manajemen AWS dari jaringan yang dikonfigurasi untuk mencapai titik akhir AWS layanan melalui titik akhir VPC.
- Anda membatasi akses ke AWS layanan dengan menggunakan `aws:SourceIp` atau kunci kondisi `aws:SourceVpc` global dalam kebijakan IAM Anda.

Kami menyarankan Anda meninjau kebijakan IAM yang berisi `aws:SourceIp` atau kunci kondisi `aws:SourceVpc` global. Terapkan keduanya `aws:SourceIp` dan `aws:SourceVpc` jika berlaku.

Beberapa Konsol Manajemen AWS fitur menggunakan domain dual-stack yang mendukung keduanya IPv4 dan koneksi. IPv6 Jika kebijakan IAM Anda membatasi akses menggunakan hanya `aws:SourceIp` dengan blok IPv4 CIDR, permintaan mungkin gagal ketika sistem operasi Anda lebih memilih IPv6 koneksi (atau sebaliknya). Untuk menghindari hal ini, sertakan keduanya IPv4 dan blok

IPv6 CIDR dalam `aws:SourceIp` kondisi Anda. Untuk informasi selengkapnya, lihat aws: SourceIp di Panduan AWS Identity and Access Management Pengguna.

Anda juga dapat melakukan onboard ke fitur Akses Konsol Manajemen AWS Pribadi untuk mengakses Konsol Manajemen AWS melalui titik akhir VPC dan kondisi `aws:SourceVpc` penggunaan dalam kebijakan Anda. Untuk informasi selengkapnya, lihat berikut ini:

- Konsol Manajemen AWS Akses Pribadi
- the section called “Bagaimana Konsol Manajemen AWS Private Access bekerja dengan aws: SourceVpc”
- the section called “Kunci konteks kondisi AWS global yang didukung”

## Browser saya menampilkan kesalahan batas waktu saat menghubungkan ke Konsol Manajemen AWS

Jika ada pemadaman layanan di default Anda Wilayah AWS, browser Anda mungkin menampilkan kesalahan 504 Gateway Timeout saat mencoba menyambung ke file. Konsol Manajemen AWS Untuk masuk ke Konsol Manajemen AWS dari Wilayah yang berbeda, tentukan titik akhir Regional alternatif di URL. Misalnya, jika terjadi pemadaman di Wilayah `us-west-1` (California Utara), untuk mengakses Wilayah `us-west-2` (Oregon) gunakan templat berikut:

```
https://region.console.aws.amazon.com
```

Untuk informasi selengkapnya, lihat titik akhir Konsol Manajemen AWS layanan di. Referensi Umum AWS

Untuk melihat status semua Layanan AWS, termasuk Konsol Manajemen AWS, lihat Dasbor AWS Health.

## Saya ingin mengubah bahasa Konsol Manajemen AWS tetapi saya tidak dapat menemukan menu pemilihan bahasa di bagian bawah halaman

Menu pemilihan bahasa telah pindah ke halaman Pengaturan Terpadu yang baru. Untuk mengubah bahasa Konsol Manajemen AWS, navigasikan ke halaman Pengaturan Terpadu, lalu pilih bahasa untuk konsol.

Untuk informasi selengkapnya, lihat Mengubah bahasa Konsol Manajemen AWS.

# Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada Panduan Konsol Manajemen AWS Memulai, mulai Maret 2021.

| Ubah | Deskripsi | Date |
| --- | --- | --- |
| Kebijakan AWS terkelola yang diperbarui | Memperbarui AWSManagementConsoleAdministratorAccessdan AWSManagementConsoleBasicUserAccesskebijakan dengan izin UXC baru. Untuk informasi selengkapnya, lihat ???. | Maret 26, 2026 |
| Halaman ditambahkan | Halaman baru ditambahkan untuk menjelaskan tindakan yang disarankan. Untuk informasi selengkapnya, lihat ???. | Oktober 15, 2025 |
| Kebijakan AWS terkelola baru | Menambahkan dua kebijakan baru ke izin cakupan untuk menggunakan, mengonfigurasi, dan menyesuaikan. Konsol Manajemen AWS<br>• AWSManagementConsoleBasicUserAccess<br>• AWSManagementConsoleAdministratorAccess | Agustus 14, 2025 |
| Kustomisasi Pengalaman Pengguna (UXC) | Layanan baru tersedia. | Agustus 14, 2025 |
| Halaman diperbarui | Anda sekarang dapat melihat aplikasi Anda di MyApplica | Juli 29, 2025 |

| Ubah | Deskripsi | Date |
| --- | --- | --- |
| | tions dari menu Layanan. Untuk informasi selengkapnya, lihat ???. | |
| Halaman ditambahkan | Halaman baru ditambahkan untuk menjelaskan fitur multisession. Untuk informasi selengkapnya, lihat ???. | Desember 6, 2024 |
| Halaman diperbarui | Mengubah halaman kata sandi Anda diperbarui. Untuk informasi selengkapnya, lihat ???. | Juni 18, 2024 |
| Halaman baru ditambahkan | Halaman baru ditambahkan untuk menjelaskan cara mengakses menu Layanan dan pemberitahuan AWS acara. Untuk informasi selengkapnya, lihat ??? dan ???. | Juni 18, 2024 |
| Halaman diperbarui | Apa itu Konsol Manajemen AWS? halaman diperbarui. Untuk informasi selengkapnya, lihat ???. | Juni 18, 2024 |
| Dapatkan dukungan | Halaman baru ditambahkan untuk menjelaskan cara mendapatkan dukungan. Untuk informasi selengkapnya, lihat ???. | Juni 18, 2024 |

| Ubah | Deskripsi | Date |
| --- | --- | --- |
| Navigasi Terpadu dan AWS Console Home | Halaman baru ditambahkan untuk menjelaskan cara bekerja dengan konsol. Untuk informasi selengkapnya, lihat ??? dan ???. | Juni 18, 2024 |
| Mengobrol dengan Amazon Q | Halaman pengaturan baru yang merinci bagaimana pengguna dapat mengajukan AWS pertanyaan kepada Pengembang Amazon Q. Untuk informasi selengkapnya, lihat Mengobrol dengan Pengembang Amazon Q. | 29 Mei 2024 |
| MyApplications | Halaman baru yang memperkenalkan MyApplications. Untuk informasi selengkapnya, lihat Apa itu MyApplications? AWS . | November 29, 2023 |
| Mengkonfigurasi Pengaturan Terpadu | Halaman pengaturan baru untuk mengonfigurasi pengaturan dan default yang berlaku untuk pengguna saat ini, termasuk bahasa dan wilayah. Untuk informasi selengkapnya, lihat Mengonfigurasi Setelan Terpadu. | April 6, 2022 |

| Ubah | Deskripsi | Date |
| --- | --- | --- |
| AWS Console Home UI baru | AWS Console Home UI baru, yang mencakup widget untuk menampilkan informasi penggunaan penting dan pintasan ke layanan. AWS Untuk informasi selengkapnya, lihat Menggunakan widget. | 25 Februari 2022 |
| Mengubah bahasa Konsol | Pilih bahasa yang berbeda untuk Konsol Manajemen AWS. Untuk informasi selengkapnya, lihat Mengubah bahasa Konsol Manajemen AWS. | 1 April 2021 |
| Peluncuran CloudShell | Buka AWS CloudShell dari Konsol Manajemen AWS dan jalankan perintah AWS CLI. Untuk informasi selengkap nya, lihat Peluncuran AWS CloudShell. | 22 Maret 2021 |

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