



Panduan Memulai

AWS Management Console



Versi 1.0

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Management Console: Panduan Memulai

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Apa itu AWS Management Console?	1
Menggunakan perangkat pilihan Anda	1
Mengkonfigurasi AWS Management Console	2
Bekerja dengan widget	2
.....	2
Mengkonfigurasi Pengaturan Terpadu	4
Mengakses Pengaturan Terpadu	4
Mengatur Ulang Pengaturan Terpadu	5
Mengedit Pengaturan Terpadu	6
Ubah mode visual AWS Management Console	7
Mengubah bahasa default di Pengaturan Terpadu	7
Memilih Wilayah	7
Menambahkan dan menghapus favorit	8
Mengubah kata sandi	9
Mengubah bahasa AWS Management Console	10
Memulai dengan layanan	12
Pencarian Terpadu	13
Mengobrol dengan Amazon Q	14
Memulai Amazon Q	14
Contoh pertanyaan	14
MyApplications pada AWS	15
Fitur MyApplications	15
Layanan terkait	16
Mengakses MyApplications	16
Harga	16
Wilayah yang Didukung	16
Wilayah Keikutsertaan	17
Memulai dengan MyApplications	18
Langkah 1: Membuat aplikasi	18
Langkah 2: Melihat aplikasi	20
Mengelola aplikasi	21
Mengedit aplikasi	21
Menghapus aplikasi	21
Membuat cuplikan kode	22

Mengelola sumber daya	22
Menambahkan sumber daya	23
Menghapus sumber daya	23
Dasbor MyApplications	24
Widget pengaturan dasbor aplikasi	24
Widget ringkasan aplikasi	24
Widget komputasi	24
Widget biaya dan penggunaan	25
AWS Widget keamanan	25
DevOps widget	26
Widget pemantauan dan operasi	26
Tag widget	27
AWS Management Console Akses Pribadi	28
Didukung Wilayah AWS, konsol layanan, dan fitur	28
Ikhtisar kontrol keamanan Akses AWS Management Console Pribadi	32
Pembatasan akun AWS Management Console dari jaringan Anda	32
Konektivitas dari jaringan Anda ke internet	32
Titik akhir VPC dan konfigurasi DNS yang diperlukan	33
DNSkonfigurasi untuk AWS Management Console dan AWS Sign-In	33
Titik akhir dan konfigurasi VPC untuk layanan DNSAWS	35
Menerapkan kebijakan kontrol layanan dan kebijakan titik akhir VPC	37
Menggunakan AWS Management Console Private Access dengan kebijakan kontrol AWS Organizations layanan	37
Izinkan AWS Management Console penggunaan hanya untuk akun dan organisasi yang diharapkan (identitas tepercaya)	37
Menerapkan kebijakan berbasis identitas dan jenis kebijakan lainnya	39
Kunci konteks kondisi AWS global yang didukung	39
Bagaimana AWS Management Console Private Access bekerja dengan aws: SourceVpc	39
Bagaimana jalur jaringan yang berbeda tercermin dalam CloudTrail	41
Coba Akses AWS Management Console Pribadi	41
Uji pengaturan dengan Amazon EC2	42
Uji pengaturan dengan Amazon WorkSpaces	56
Uji pengaturan VPC dengan kebijakan IAM	73
Arsitektur referensi	75
PeluncuranAWS CloudShell di Toolbar Konsol	77
Mendapatkan informasi penagihan	78

Penurunan harga di AWS	79
Paragraf, Spasi Baris, dan Garis Horizontal	79
Judul	80
Format Teks	80
Tautan	81
Daftar	81
Tabel dan Tombol (CloudWatch Dasbor)	81
Pemecahan Masalah	83
Halaman tidak dimuat dengan benar	83
Browser saya menampilkan kesalahan 'akses ditolak' saat menghubungkan ke AWS Management Console	84
Browser saya menampilkan kesalahan batas waktu saat menghubungkan ke AWS Management Console	85
Saya ingin mengubah bahasa AWS Management Console tetapi saya tidak dapat menemukan menu pemilihan bahasa di bagian bawah halaman	85
Riwayat dokumen	86
AWSGlosarium	88
.....	lxxxix

Apa itu AWS Management Console?

[AWS Management Console](#) Ini adalah aplikasi web yang terdiri dan mengacu pada koleksi luas konsol layanan untuk mengelola AWS sumber daya. Saat pertama kali masuk, Anda akan melihat halaman beranda konsol. Halaman beranda menyediakan akses ke setiap konsol layanan dan menawarkan satu tempat untuk mengakses informasi yang Anda butuhkan untuk melakukan tugas AWS terkait Anda. Ini juga memungkinkan Anda menyesuaikan pengalaman Console Home dengan menambahkan, menghapus, dan mengatur ulang widget seperti Baru-baru ini dikunjungi, AWS Kesehatan, dan banyak lagi.

Note

Opsi pemilihan bahasa telah pindah ke halaman Pengaturan Terpadu yang baru. Untuk informasi selengkapnya, lihat [Mengubah bahasa AWS Management Console](#).

Konsol layanan individual, di sisi lain, menawarkan berbagai alat untuk komputasi awan, serta informasi tentang akun Anda dan tentang [penagihan](#) Anda.

Menggunakan perangkat pilihan Anda

[AWS Management Console](#) telah dirancang untuk berfungsi pada tablet serta jenis perangkat 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.

AWS Management Console Ini juga tersedia sebagai aplikasi untuk Android dan iOS. Aplikasi ini menyediakan tugas-tugas yang relevan dengan perangkat seluler yang merupakan pendamping yang baik untuk pengalaman web secara keseluruhan. Misalnya, Anda dapat dengan mudah melihat dan mengelola instans Amazon EC2 dan CloudWatch alarm Amazon yang ada dari ponsel Anda.

Anda dapat mengunduh aplikasi seluler AWS Konsol dari [Amazon Appstore](#), [Google Play](#), atau [iTunes](#).

Mengkonfigurasi AWS Management Console

Topik ini menjelaskan cara mengonfigurasi Anda AWS Management Console dan cara menggunakan halaman Setelan Terpadu untuk menetapkan default yang berlaku untuk semua konsol layanan. Ini juga menjelaskan widget, fitur dasbor Beranda Konsol yang memungkinkan Anda menambahkan komponen khusus yang melacak informasi tentang AWS layanan dan sumber daya Anda.

Topik

- [Bekerja dengan widget](#)
- [Mengkonfigurasi Pengaturan Terpadu](#)
- [Memilih Wilayah](#)
- [Menambahkan dan menghapus favorit](#)
- [Mengubah kata sandi](#)
- [Mengubah bahasa AWS Management Console](#)

Bekerja dengan widget

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.

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 menyiapkan widget, 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. AWS Management Console

Mengkonfigurasi Pengaturan Terpadu

Anda dapat mengonfigurasi pengaturan dan default, seperti tampilan, bahasa, dan Wilayah, dari halaman Pengaturan AWS Management Console Terpadu. Mode visual dan bahasa default juga dapat diatur langsung dari bilah navigasi. Perubahan ini berlaku untuk semua konsol layanan.

Important

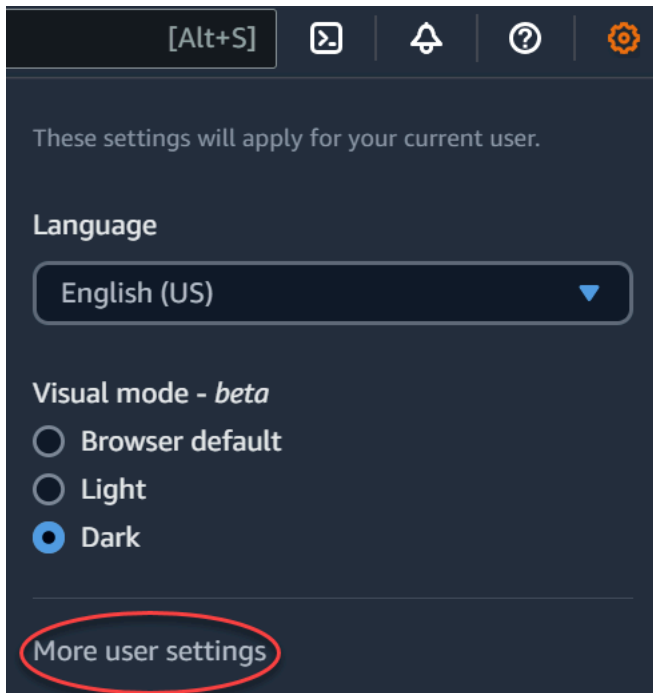
Untuk memastikan bahwa pengaturan, layanan favorit, dan layanan yang baru dikunjungi tetap ada secara global, data ini disimpan di semua Wilayah AWS, termasuk Wilayah yang dinonaktifkan secara default. Wilayah tersebut adalah Afrika (Cape Town), Asia Pasifik (Hong Kong), Asia Pasifik (Hyderabad), Asia Pasifik (Jakarta), Eropa (Milan), Eropa (Spanyol), Eropa (Zurich), Timur Tengah (Bahrain), dan Timur Tengah (UEA). Anda masih perlu [mengaktifkan Region 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.

Mengakses Pengaturan Terpadu

Prosedur berikut menjelaskan cara mengakses Pengaturan Terpadu.

Untuk mengakses Setelan Terpadu

1. Masuk ke [AWS Management Console](#).
2. Di bilah navigasi, pilih ikon roda gigi.
3. Untuk membuka halaman Pengaturan Terpadu, pilih Pengaturan pengguna lainnya.



Mengatur Ulang Pengaturan Terpadu

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

Note

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 [AWS Management Console](#).
2. Di bilah navigasi, pilih ikon roda gigi.
3. Buka halaman Pengaturan Terpadu dengan memilih Pengaturan pengguna lainnya.
4. Pilih Atur Ulang semua.

Mengedit Pengaturan Terpadu

Prosedur berikut menjelaskan cara mengedit pengaturan pilihan Anda.

Untuk mengedit Setelan Terpadu

1. Masuk ke [AWS Management Console](#).
2. Di bilah navigasi, pilih ikon roda gigi.
3. Buka halaman Pengaturan Terpadu dengan memilih Pengaturan pengguna lainnya.
4. Pilih Edit di samping pengaturan pilihan Anda:
 - Lokalisasi dan Wilayah default:
 - Bahasa memungkinkan Anda memilih bahasa default untuk teks konsol.
 - Default Region memungkinkan Anda memilih Region default yang berlaku setiap kali Anda login. 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 [AWS Management Console](#), 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 AWS Management Console 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.

Ubah mode visual AWS Management Console

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 [AWS Management Console](#).
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.

Mengubah bahasa default di Pengaturan Terpadu

Prosedur berikut menjelaskan cara mengubah bahasa default menggunakan bilah navigasi.

Untuk mengubah bahasa default dari bilah navigasi

1. Masuk ke [AWS Management Console](#).
2. Di bilah navigasi, pilih ikon roda gigi.
3. Untuk Bahasa, pilih Browser default atau bahasa pilihan dari daftar dropdown.

Memilih Wilayah

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 [AWS Management Console](#) atau untuk beberapa layanan, seperti AWS Identity and Access Management. Untuk mempelajari selengkapnya Wilayah AWS, lihat [Mengelola Wilayah AWS](#) di Referensi Umum AWS.

Untuk memilih Wilayah

1. Masuk ke [AWS Management Console](#).
2. [Pilih layanan](#) untuk pergi ke konsol layanan itu.
3. Di bilah navigasi, pilih nama Wilayah yang saat ini ditampilkan. Kemudian pilih Wilayah yang ingin Anda alihkan.

Untuk memilih Region default

1. Di bilah navigasi, pilih ikon pengaturan, lalu pilih Pengaturan pengguna lainnya untuk menavigasi ke halaman Pengaturan Terpadu.
2. Pilih Edit di samping Lokalisasi dan Wilayah default.
3. Pilih Wilayah default Anda, lalu pilih Simpan pengaturan. Jika Anda tidak memilih Wilayah default, Wilayah terakhir yang Anda kunjungi akan menjadi default Anda.
4. (Opsional) Pilih Pergi ke Wilayah default baru untuk segera pergi ke Wilayah default baru Anda.

Note

Jika Anda telah membuat AWS sumber daya tetapi 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. Untuk melihatnya, gunakan pemilih Wilayah untuk memilih Wilayah yang berisi sumber daya Anda.

Menambahkan dan menghapus favorit

Untuk mengakses layanan yang sering Anda gunakan lebih cepat, Anda dapat menyimpan konsol layanan mereka ke daftar Favorit.

Untuk menambahkan layanan ke daftar Favorit

1. Masuk ke [AWS Management Console](#).
2. Pilih tombol Tambah widget di sisi kanan atas atau bawah halaman.
3. Di menu Tambah widget, pilih Favorit untuk ditambahkan ke konsol, lalu pilih Tambah.

Favorit akan ditambahkan ke bagian bawah Rumah Konsol Anda. Anda dapat menarik dan melepas Favorit dengan memilih bilah judul di bagian atas widget, lalu seret widget ke lokasi baru di halaman.

4. Di bilah navigasi, pilih Layanan.
5. Baik dalam daftar yang baru dikunjungi atau daftar Semua layanan, arahkan kursor ke nama layanan yang ingin Anda tambahkan sebagai favorit.
6. Pilih bintang di sebelah kiri nama layanan.

7. Ulangi dua langkah sebelumnya untuk menambahkan lebih banyak layanan ke daftar Favorit.

Untuk menghapus layanan dari daftar Favorit

1. Di bilah navigasi, pilih Layanan.
2. Lakukan salah satu hal berikut ini:
 - Dalam daftar Favorit, arahkan kursor ke nama layanan. Kemudian pilih × di sebelah kanan nama layanan.
 - Di daftar Baru saja dikunjungi atau daftar Semua layanan, batalkan pilihan bintang pada nama layanan yang ada di daftar Favorit Anda.

Mengubah kata sandi

Jika Anda adalah pemilik akun, Anda dapat mengubah kata sandi AWS akun Anda dari [AWS Management Console](#).

Untuk mengubah kata sandi

1. Masuk ke [AWS Management Console](#).
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.

Mengubah bahasa AWS Management Console

AWS Console Home Pengalaman mencakup halaman Pengaturan Terpadu tempat Anda dapat mengubah bahasa default untuk AWS layanan di AWS Management Console. Anda juga dapat mengubah bahasa default dengan cepat dari menu pengaturan, yang dapat Anda akses dari bilah navigasi. Anda dapat membuat perubahan ini dari mana saja di konsol.

Note

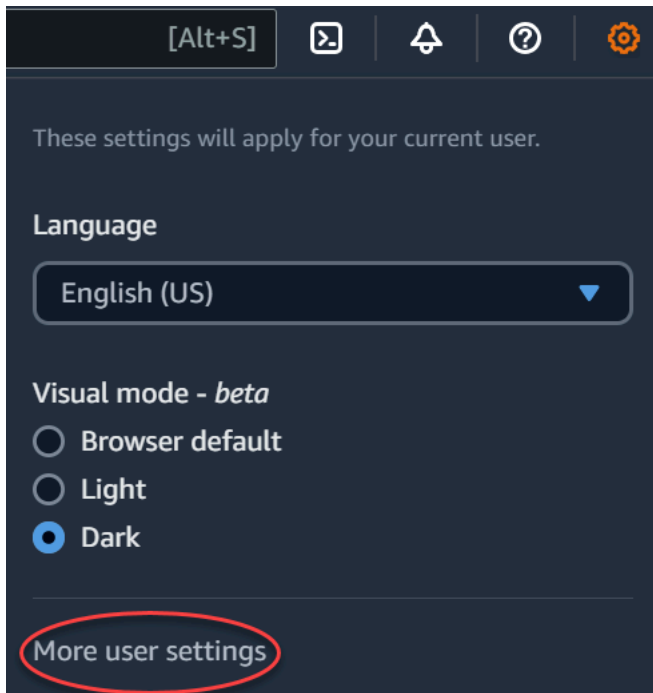
Prosedur ini mengubah bahasa untuk semua konsol, tetapi tidak untuk AWS dokumentasi. Untuk mengubah bahasa yang digunakan untuk dokumentasi, gunakan menu bahasa di kanan atas halaman dokumentasi apa pun.

AWS Management Console Saat ini mendukung bahasa berikut:

- Inggris (US)
- Inggris (UK)
- Bahasa Indonesia
- Bahasa Jerman
- Prancis
- Bahasa Jepang
- Bahasa Spanyol
- Bahasa Italia
- Bahasa Portugis
- Bahasa Korea
- Mandarin (Sederhana)
- Mandarin (Tradisional)

Untuk mengubah bahasa default di Pengaturan Terpadu

1. Masuk ke [AWS Management Console](#).
2. Di bilah navigasi, pilih ikon pengaturan.
3. Untuk membuka halaman Pengaturan Terpadu, pilih Pengaturan pengguna lainnya.



4. Di Pengaturan Terpadu, pilih Edit di samping Lokasi 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 AWS Management Console.

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

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

Untuk mengubah bahasa default dari bilah navigasi

1. Masuk ke [AWS Management Console](#).
2. Di bilah navigasi, pilih ikon pengaturan.
3. Untuk Bahasa, pilih salah satu Browser default atau bahasa pilihan dari daftar dropdown.

Memulai dengan layanan

[AWS Management Console](#) menyediakan beberapa cara untuk menavigasi ke konsol tiap-tiap layanan.

Untuk membuka konsol sebuah layanan

Lakukan salah satu dari berikut:

- 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 Layanan yang baru saja dikunjungi widget, pilih nama layanan.
- Di Layanan yang baru saja dikunjungi widget, pilih Lihat semua AWS jasa. Kemudian, pada Semua AWS jasa halaman, pilih nama layanan.
- Di bilah navigasi, pilih Layanan untuk membuka daftar lengkap layanan. Lalu pilih layanan dari daftar Baru saja dikunjungi atau Semua layanan.

Mencari produk, layanan, fitur, dan lainnya menggunakan Unified Search

Kotak pencarian di bilah navigasi menyediakan alat pencarian terpadu untuk melacak layanan dan fitur AWS, dokumentasi layanan, dan AWS Marketplace. Cukup ketik beberapa karakter untuk melihat hasil dari semua kategori ini. Semakin banyak karakter yang Anda ketik, semakin sesuai hasil pencarian Anda.

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

1. Di kotak pencarian di bilah navigasi AWS Management Console, masukkan semua atau sebagian istilah pencarian Anda.
2. Lakukan salah satu hal berikut untuk menyempurnakan pencarian Anda dan mendapatkan lebih banyak detail:
 - Untuk mempersempit hasil menjadi jenis konten yang Anda inginkan, pilih salah satu kategori di sebelah kiri.
 - Untuk melihat lebih banyak hasil dari kategori tertentu, pilih Lihat keseluruhan **n** hasil pada setiap judul kategori. Untuk kembali ke daftar hasil utama, pilih Kembali di pojok kiri atas.
 - Untuk menavigasi ke fitur populer layanan dengan cepat, beri jeda pada nama layanan pada hasil dan pilih tautan.
 - Untuk mendapatkan detail lebih lanjut tentang dokumentasi atau AWS Marketplace hasil, jeda pada judul hasil.
3. Pilih tautan untuk mengarahkan ke layanan, topik, atau halaman AWS Marketplace 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.

Mengobrol dengan Pengembang Amazon Q

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 AWS Management Console, 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?

Apa itu MyApplications? AWS

MyApplications adalah perpanjangan dari Console Home yang membantu Anda mengelola dan memantau biaya, kesehatan, postur keamanan, dan kinerja aplikasi Anda. AWS 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 AWS Management Console. 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

Fitur MyApplications

- **Buat aplikasi** — Buat aplikasi baru dan atur sumber dayanya. Aplikasi Anda secara otomatis ditampilkan di MyApplications, sehingga Anda dapat mengambil tindakan di AWS Management Console, API, CLI, dan SDK. 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.
- **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, 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
- Systems Manager
- AWS Service Catalog
- Penandaan

Mengakses MyApplications

Anda dapat mengakses MyApplications dari [AWS Management Console](#) dengan 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

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:

- Afrika (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)

Memulai dengan MyApplications

Untuk mulai menggunakan MyApplications untuk membuat, memantau, dan mengendalikan aplikasi Anda, gunakan langkah-langkah berikut.

Langkah 1: Membuat aplikasi

Buat aplikasi baru atau gunakan aplikasi yang sudah ada yang dibuat sebelum 8 November 2023 untuk memulai dengan AppRegistry MyApplications.

Create an application

Untuk membuat aplikasi

1. Masuk ke [AWS Management Console](#).
2. Di sidebar kiri, 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 dan dapat digunakan untuk mengidentifikasi sumber daya yang terkait dengan aplikasi Anda. 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 Selanjutnya.
9. (Opsional) Tambahkan sumber daya yang ada:

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.

- a. Pilih Pilih sumber daya.
- b. (Opsional) Pilih [tampilan](#).
- c. 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.

- d. Pilih kotak centang di sebelah sumber daya yang ingin Anda tambahkan.
 - e. Pilih Tambahkan.
 - f. Pilih Selanjutnya.
10. Tinjau pilihan Anda.
 11. Jika mengaitkan AWS CloudFormation tumpukan, pilih kotak centang di bagian bawah halaman.

Note

Menambahkan AWS 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 AWS CloudFormation Pengguna.

12. Pilih Create application (Buat aplikasi).

Onboard existing application

Untuk onboard aplikasi yang ada AppRegistry

1. Masuk ke [AWS Management Console](#).
2. Di sidebar kiri, pilih MyApplications.
3. Gunakan bilah pencarian untuk menemukan aplikasi Anda.
4. Pilih aplikasi Anda.
5. Pilih **nama aplikasi** Onboard.
6. Jika mengaitkan CloudFormation tumpukan, pilih kotak centang di kotak peringatan.
7. Pilih aplikasi Onboard.

Langkah 2: Melihat aplikasi

Anda dapat melihat aplikasi Anda di semua Wilayah atau Wilayah tertentu dan informasi yang relevan dalam tampilan kartu atau tabel.

Untuk melihat aplikasi

1. Di sidebar kiri, pilih MyApplications.
2. Di Wilayah, pilih Wilayah Saat Ini atau Wilayah yang Didukung.
3. Untuk menemukan aplikasi tertentu, masukkan nama, kata kunci, atau deskripsi di bilah pencarian.
4. (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.

Mengelola aplikasi

Topik ini mencakup bagaimana Anda dapat mengelola aplikasi Anda.

Mengedit aplikasi

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 [AWS Management Console](#).
2. Di bilah sisi kiri konsol, pilih MyApplications.
3. Pilih aplikasi yang ingin Anda edit.
4. Pada dasbor MyApplication, Pilih Tindakan dan kemudian pilih Edit aplikasi.
5. Di Edit deskripsi aplikasi, perbarui deskripsi, lalu pilih Simpan perubahan.

Untuk mengedit tag

- Ikuti langkah-langkah dalam [Mengelola tag](#) di Panduan AWS Service Catalog AppRegistry Administrator.

Untuk mengedit grup atribut

- Ikuti langkah-langkah dalam [Mengedit grup atribut](#) di Panduan AWS Service Catalog AppRegistry Administrator.

Menghapus aplikasi

Anda dapat menghapus aplikasi jika tidak lagi diperlukan.

Untuk menghapus aplikasi

1. Buka [AWS Management Console](#).
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. Pilih Hapus.
7. Konfirmasikan penghapusan Anda, lalu pilih Hapus aplikasi.

Membuat cuplikan kode

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 [AWS Management Console](#).
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.

Mengelola sumber daya

Topik ini mencakup cara mengelola sumber daya Anda.

Menambahkan sumber daya

Menambahkan sumber daya ke aplikasi Anda memungkinkan Anda mengelompokkannya dan mengelola keamanan, kinerja, dan kepatuhannya.

Untuk menambahkan sumber daya

1. Buka [AWS Management Console](#).
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.

Menghapus sumber daya

Anda dapat menghapus sumber daya untuk memisahkannya dari aplikasi Anda.

Untuk menghapus sumber daya

1. Buka [AWS Management Console](#).
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.

Dasbor MyApplications

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](#).

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 dicampur dan diperbarui setidaknya sekali setiap 24 jam. Untuk 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](#).

Mengkonfigurasi widget AWS Keamanan

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

AWS Security Hub 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.

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 wawasan 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 (kekritisannya, lingkungan, pusat biaya). Untuk informasi selengkapnya, lihat [Apa itu tag?](#) dalam Praktik terbaik untuk Menandai AWS Sumber Daya AWS Whitepaper.

AWS Management Console Akses Pribadi

AWS Management Console Private Access adalah fitur keamanan canggih untuk mengontrol akses ke AWS Management Console. AWS Management Console Akses Pribadi berguna ketika Anda ingin mencegah pengguna masuk ke tak terduga Akun AWS dari dalam jaringan Anda. Dengan fitur ini, Anda dapat membatasi akses ke AWS Management Console satu-satunya ke set tertentu yang diketahui Akun AWS ketika lalu lintas berasal dari dalam jaringan Anda.

Topik

- [Didukung Wilayah AWS, konsol layanan, dan fitur](#)
- [Ikhtisar kontrol keamanan Akses AWS Management Console 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 AWS Management Console Pribadi](#)
- [Arsitektur referensi](#)

Didukung Wilayah AWS, konsol layanan, dan fitur

AWS Management Console Private Access hanya mendukung sebagian Wilayah dan AWS layanan. Konsol layanan yang tidak didukung akan tidak aktif di. AWS Management Console Selain itu, AWS Management Console fitur tertentu mungkin dinonaktifkan saat menggunakan Akses AWS Management Console 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 (Tokyo)
- Kanada (Pusat)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Paris)
- Eropa (Stockholm)
- Amerika Selatan (Sao Paulo)
- Afrika (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Melbourne)
- Kanada Barat (Calgary)
- Eropa (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

- Amazon Athena
- AWS Auto Scaling
- AWS Billing Conductor
- AWS Certificate Manager
- AWS Cloud Map
- Amazon CloudFront
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Database Migration Service
- AWS DeepRacer
- 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
- Amazon ElastiCache
- Amazon EMR

- Amazon EventBridge
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- 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 Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- 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 Manager
- OpenSearch Layanan Amazon
- AWS Organizations
- Amazon S3 di Outposts
- SageMaker Runtime Amazon

- Data SageMaker Sintetis Amazon
- AWS Secrets Manager
- Service Quotas
- AWS Signer
- Layanan Email Sederhana Amazon
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- Pengaturan Terpadu
- Pengelola Alamat IP Amazon VPC

Ikhtisar kontrol keamanan Akses AWS Management Console Pribadi

Pembatasan akun AWS Management Console dari jaringan Anda

AWS Management Console Akses Pribadi berguna dalam skenario ketika Anda ingin membatasi akses ke AWS Management Console 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 AWS Management Console 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 AWS Management Console, seperti konten statis (JavaScript, CSS, gambar), dan semua yang Layanan AWS tidak diaktifkan oleh [AWS PrivateLink](#). Untuk daftar domain tingkat atas yang digunakan oleh AWS Management Console, lihat. [Pemecahan Masalah](#)

Note

Saat ini, AWS Management Console Private Access tidak mendukung endpoint seperti `status.aws.amazon.com`, `health.aws.amazon.com`, `dandocs.aws.amazon.com`. Anda perlu merutekan domain ini ke internet publik.

Titik akhir VPC dan konfigurasi DNS yang diperlukan

AWS Management Console Akses Pribadi memerlukan dua titik akhir VPC berikut per Wilayah. Ganti *wilayah* dengan informasi Wilayah Anda sendiri.

1. `com.amazonaws.region.console` untuk AWS Management Console
2. `com.amazonaws.region.signin` untuk AWS Sign-In

Note

Selalu sediakan infrastruktur dan konektivitas jaringan ke Wilayah AS Timur (Virginia N.) (`us-east-1`), terlepas dari Wilayah lain yang Anda gunakan dengan. AWS Management Console 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 [VPC Amazon ke Amazon VPC di whitepaper Opsi Konektivitas](#) Amazon Virtual Private Cloud.

DNS konfigurasi untuk AWS Management Console dan AWS Sign-In

Untuk merutekan lalu lintas jaringan Anda ke titik akhir VPC masing-masing, konfigurasi DNS catatan di jaringan tempat pengguna Anda akan mengakses file. AWS Management Console DNS Catatan 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:

- CNAMECatatan regional (di semua Wilayah)
- `region.signin.aws.amazon.com` menunjuk ke titik akhir VPC di zona masuk AWS Sign-In DNS
- `region.console.aws.amazon.com` menunjuk ke titik akhir VPC di zona konsol AWS Management Console 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 AWS Management Console 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 AWS Management Console 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 AWS Management Console Pribadi.

jsonFile 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-southeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ca-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 AWS Management Console Pribadi. Untuk menjaga zona host pribadi Anda diperbarui, tarik daftar file sebelumnya secara berkala.

Jika Anda menggunakan Route 53 untuk mengkonfigurasi AndaDNS, buka [#https://console.aws.amazon.com/route53/v2/hostedzones #](https://console.aws.amazon.com/route53/v2/hostedzones) untuk memverifikasi DNS pengaturan. 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.signin.aws.amazon.com
- support.console.aws.amazon.com
- global.console.aws.amazon.com
- Catatan tambahan hadir dalam file JSON yang terdaftar sebelumnya

Titik akhir dan konfigurasi VPC untuk layanan DNSAWS


AWS Management Console Panggilan Layanan AWS melalui kombinasi permintaan browser langsung dan permintaan yang diproksi oleh server web. Untuk mengarahkan lalu lintas ini ke

titik akhir AWS Management Console 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-southeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ca-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 AWS Management Console 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 (SCP) dan kebijakan titik akhir VPC AWS Management Console untuk Akses Pribadi untuk membatasi kumpulan akun yang diizinkan menggunakan AWS Management Console dari dalam VPC dan jaringan lokal yang terhubung.

Menggunakan AWS Management Console 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 AWS Management Console 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 AWS Management Console Pribadi.

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

Untuk informasi selengkapnya tentang SCP, lihat [Kebijakan kontrol layanan \(SCP\)](#) dalam Panduan Pengguna AWS Organizations .

Izinkan AWS Management Console penggunaan hanya untuk akun dan organisasi yang diharapkan (identitas tepercaya)

AWS Management Console 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 AWS Management Console 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxxx"
        }
      }
    }
  ]
}
```

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

```
{
```

```
"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 AWS Management Console 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 AWS Management Console Pribadi.

Kunci konteks kondisi AWS global yang didukung

AWS Management Console 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 AWS Management Console Pribadi.

Bagaimana AWS Management Console Private Access bekerja dengan `aws: SourceVpc`

Bagian ini menjelaskan berbagai jalur jaringan yang AWS Management Console 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 AWS Management Console web ke. Layanan AWS Implementasi ini dapat berubah sewaktu-waktu 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. AWS Management Console Selain itu, Anda harus menggunakan kondisi `aws:SourceVpc` IAM dalam kebijakan Anda daripada `aws:SourceVpce` nilai tertentu dengan fitur Akses AWS Management Console Pribadi. Bagian ini memberikan rincian tentang cara kerja jalur jaringan yang berbeda.

Setelah pengguna masuk ke AWS Management Console, mereka membuat permintaan Layanan AWS melalui kombinasi permintaan browser langsung dan permintaan yang diproksi oleh server AWS Management Console 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 AWS Management Console 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 untuk `com.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 AWS Management Console 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 konfigurasi 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 AWS Management Console 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 AWS Management Console 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. AWS Management Console `aws:SourceVpc` kondisi akan disetel ke ID titik akhir VPC login atau konsol masing-masing.

Note

Jika pengguna Anda memerlukan akses ke konsol layanan yang tidak didukung oleh Akses AWS Management Console 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 AWS Management Console tercermin dalam riwayat CloudTrail acara Anda.

Untuk permintaan browser langsung, menggunakan Akses AWS Management Console 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 AWS Management Console 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 AWS Management Console Pribadi

Bagian ini menjelaskan cara mengatur dan menguji Akses AWS Management Console Pribadi di akun baru.

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

Topik

- [Uji pengaturan dengan Amazon EC2](#)
- [Uji pengaturan dengan Amazon WorkSpaces](#)

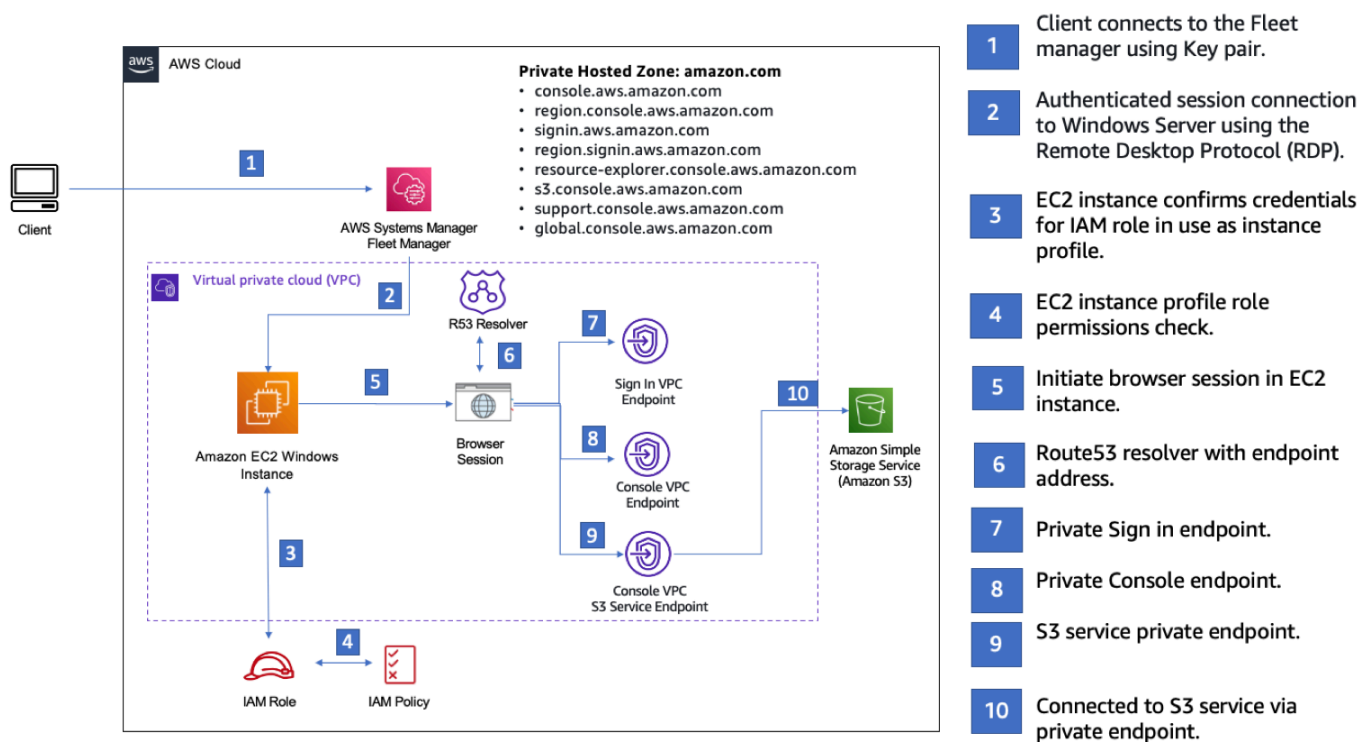
- [Uji pengaturan VPC dengan kebijakan IAM](#)

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 AWS Management Console Pribadi ke Amazon Simple Storage Service dari instans Amazon EC2. Tutorial ini digunakan AWS 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 persiapan Akses AWS Management Console Pribadi. Ini menunjukkan bagaimana pengguna terhubung ke Amazon S3 menggunakan titik akhir pribadi.



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

 Note

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

AWS Management Console Template Amazon AWS 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: 't2.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

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

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 [AWS CloudFormation konsol](#).
2. Pilih Buat tumpukan.
3. Pilih Dengan sumber daya baru (standar). Unggah file AWS 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 Sumber Daya 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. AWS CloudFormation Kemudian pilih Connect.

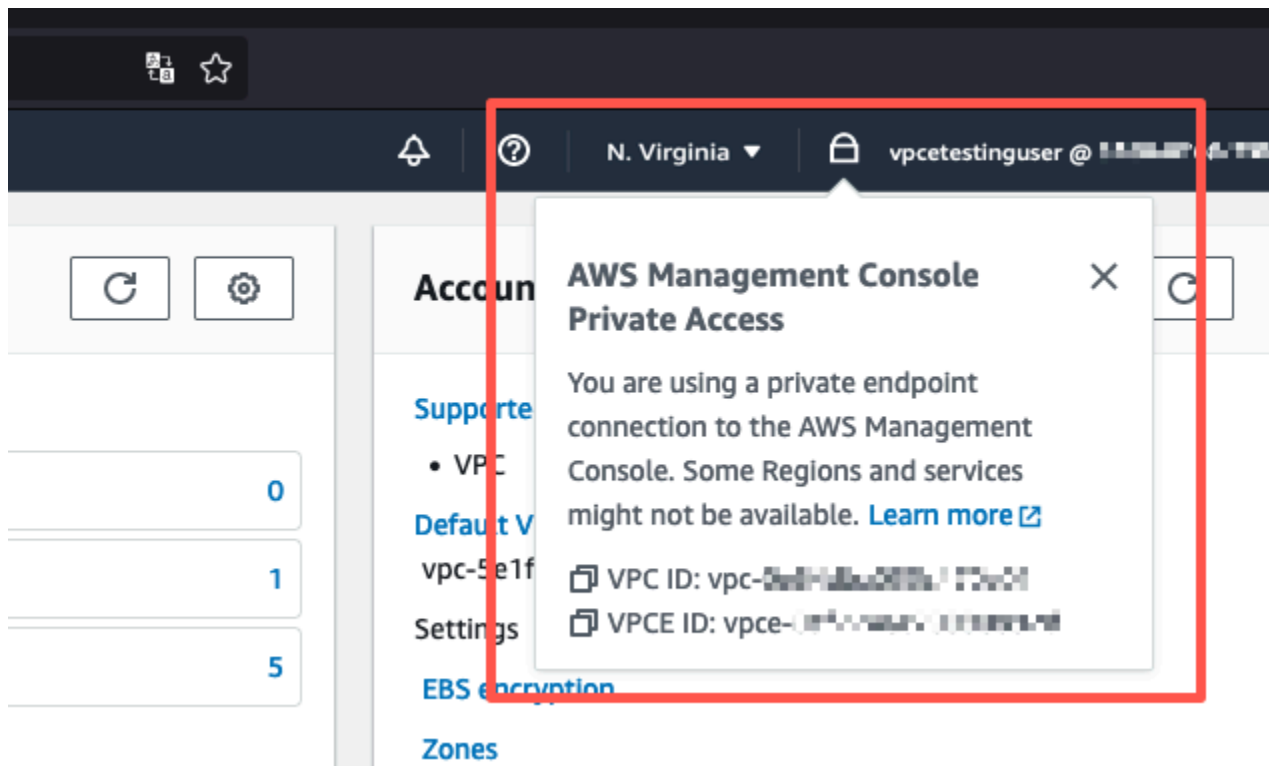
 Note

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 AWS CloudFormation membuat template.
7. Dari instans Windows Amazon EC2, buka AWS Management Console di browser.
8. Setelah Anda masuk dengan AWS kredensi Anda, buka konsol [Amazon S3](#) dan verifikasi bahwa Anda terhubung AWS Management Console menggunakan Akses Pribadi.

Untuk menguji pengaturan Akses AWS Management Console 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](#).

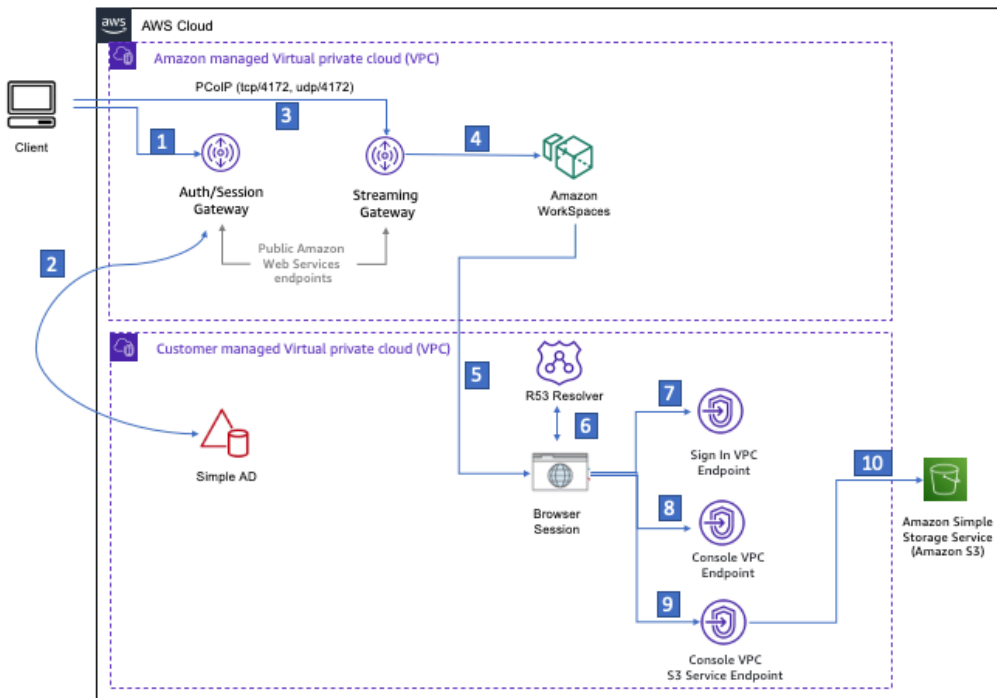
Contoh di bagian ini menjelaskan lingkungan pengujian di mana lingkungan pengguna menggunakan browser web yang berjalan pada WorkSpace untuk masuk ke Akses AWS Management Console Pribadi. Kemudian, pengguna mengunjungi konsol Amazon Simple Storage Service. Ini WorkSpace dimaksudkan untuk mensimulasikan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

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 AWS Management Console.

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

Private Hosted Zone: amazon.com

- console.aws.amazon.com
- region.console.aws.amazon.com
- signin.aws.amazon.com
- region.signin.aws.amazon.com
- resource-explorer.console.aws.amazon.com
- s3.console.aws.amazon.com
- support.console.aws.amazon.com
- global.console.aws.amazon.com



- 1 Login information sent to authentication gateway
- 2 Authentication against Simple AD
- 3 Streaming Traffic to Streaming gateway
- 4 Each WorkSpace is connected to two networks simultaneously, Amazon-managed VPC for streaming traffic and Customer managed VPC handling all other traffic.
- 5 Initiate browser session
- 6 Route53 resolver with endpoint address.
- 7 Private Sign in endpoint
- 8 Private Console endpoint
- 9 S3 service private endpoint
- 10 Connected to S3 service via private endpoint

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

AWS Management Console 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

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::VPCEGatewayAttachment
```

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

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

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: "ADAdminSecret"

Description: "Password for directory services admin"

GenerateSecretString:

SecretStringTemplate: '{"username": "Admin"}'

GenerateStringKey: password


```
PasswordLength: 30
ExcludeCharacters: '"@/\'
```

WorkspaceSimpleDirectory:

```
Type: AWS::DirectoryService::SimpleAD
```

```
DependsOn: AppVPC
```

```
DependsOn: PrivateSubnetA
```

```
DependsOn: PrivateSubnetB
```

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 [AWS CloudFormation konsol](#).
2. Pilih Buat tumpukan.
3. Pilih Dengan sumber daya baru (standar). Unggah file AWS 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 Sumber Daya 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.

PrivateConsoleNetworkForS3



Delete

Update

Stack actions ▾

Create stack ▾

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Outputs (4)

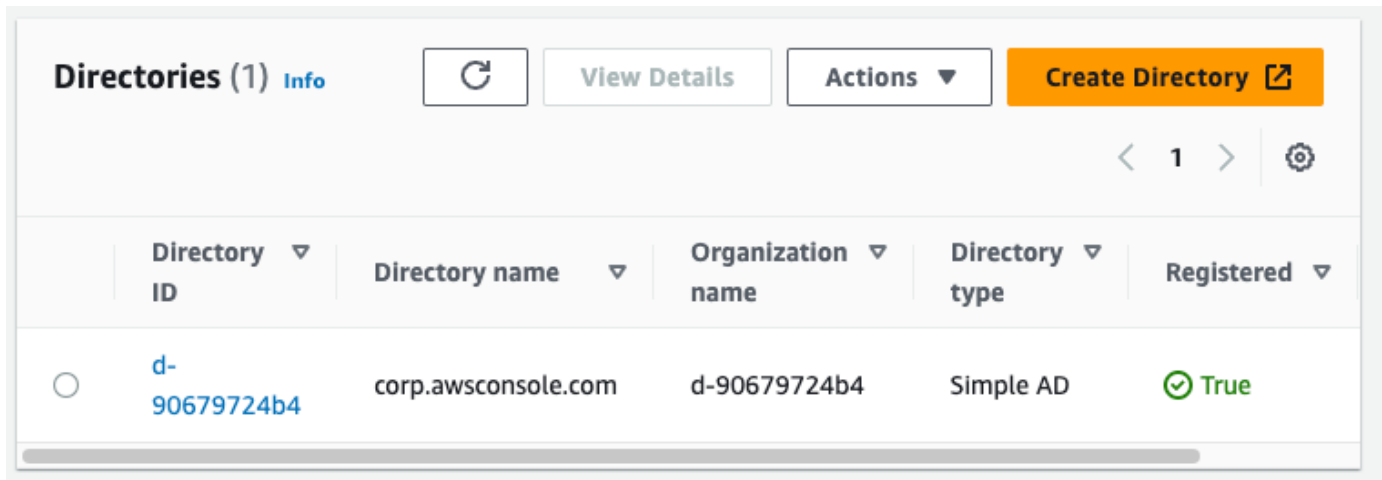


Key ▲	Value ▼	Description ▼	Export name
PrivateSubnetA	subnet-0dbb336fdb5467891	Private Subnet A	-
PrivateSubnetB	subnet-00ad943c5d84fd13a	Private Subnet B	-
WorkspacesAdminPassword	arn:aws:secretsmanager:us-east-1:425341151473:secret:ADAdminSecret-HR1MHT	The ARN of the Workspaces admin's password. Navigate to the Secrets Manager in the AWS Console to view the value.	-
WorkspaceSimpleDirectory	d-90679724b4	Directory to be used for Workspaces	-

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.



Directory ID	Directory name	Organization name	Directory type	Registered
d-90679724b4	corp.awsconsole.com	d-90679724b4	Simple AD	True

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 AWS 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 Selanjutnya.
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 AWS Management Console 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 kredensial yang Anda buat di langkah ketiga.

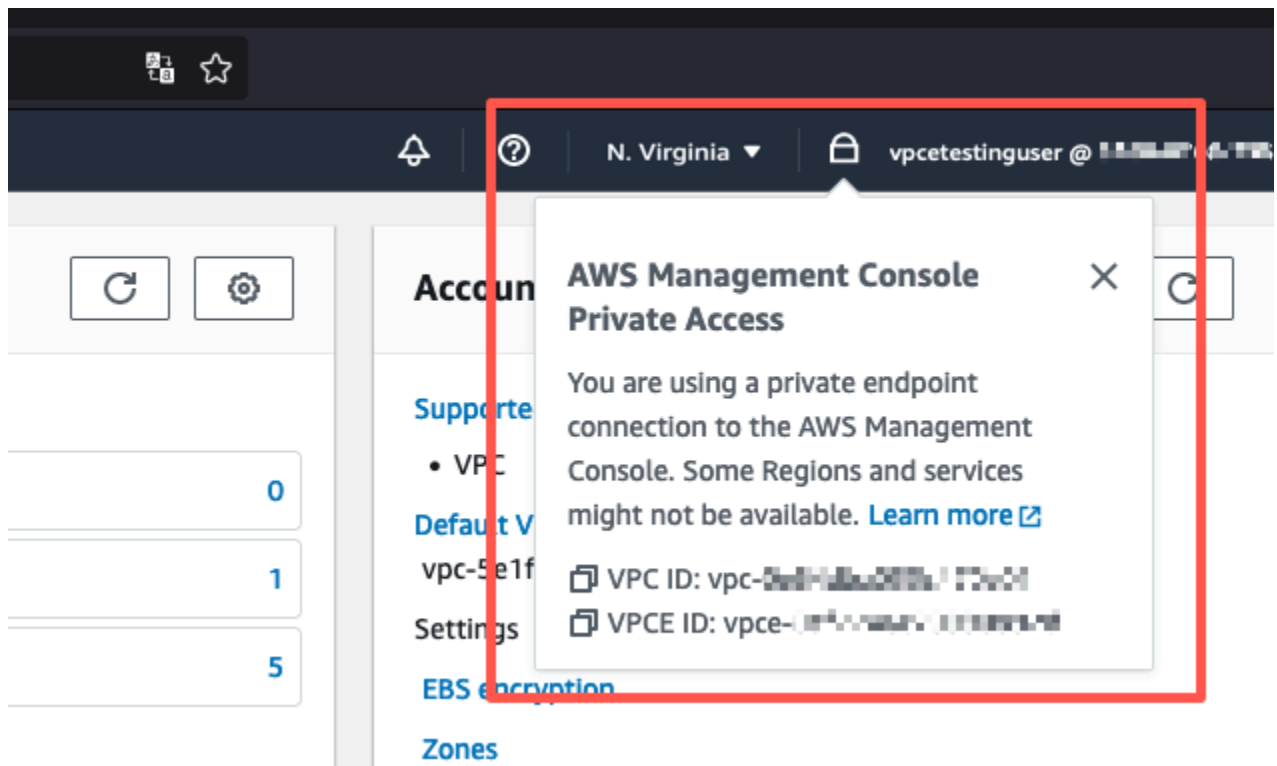
Untuk menguji pengaturan Akses AWS Management Console Pribadi

1. Dari Anda WorkSpace, buka browser Anda. Kemudian, navigasikan ke [AWS Management Console](#) dan masuk menggunakan kredensial 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 AWS Management Console 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 disiapkan 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.

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

```
}  
]  
}
```

Kebijakan berikut membatasi login ke Akun AWS ID yang dipilih menggunakan kebijakan Akses AWS Management Console Pribadi untuk titik akhir login.

```
{  
  "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.



Your account doesn't have permission to use AWS Management Console Private Access

Your corporate network uses AWS Management Console Private Access, which only allows sign-ins from specific authorized accounts.

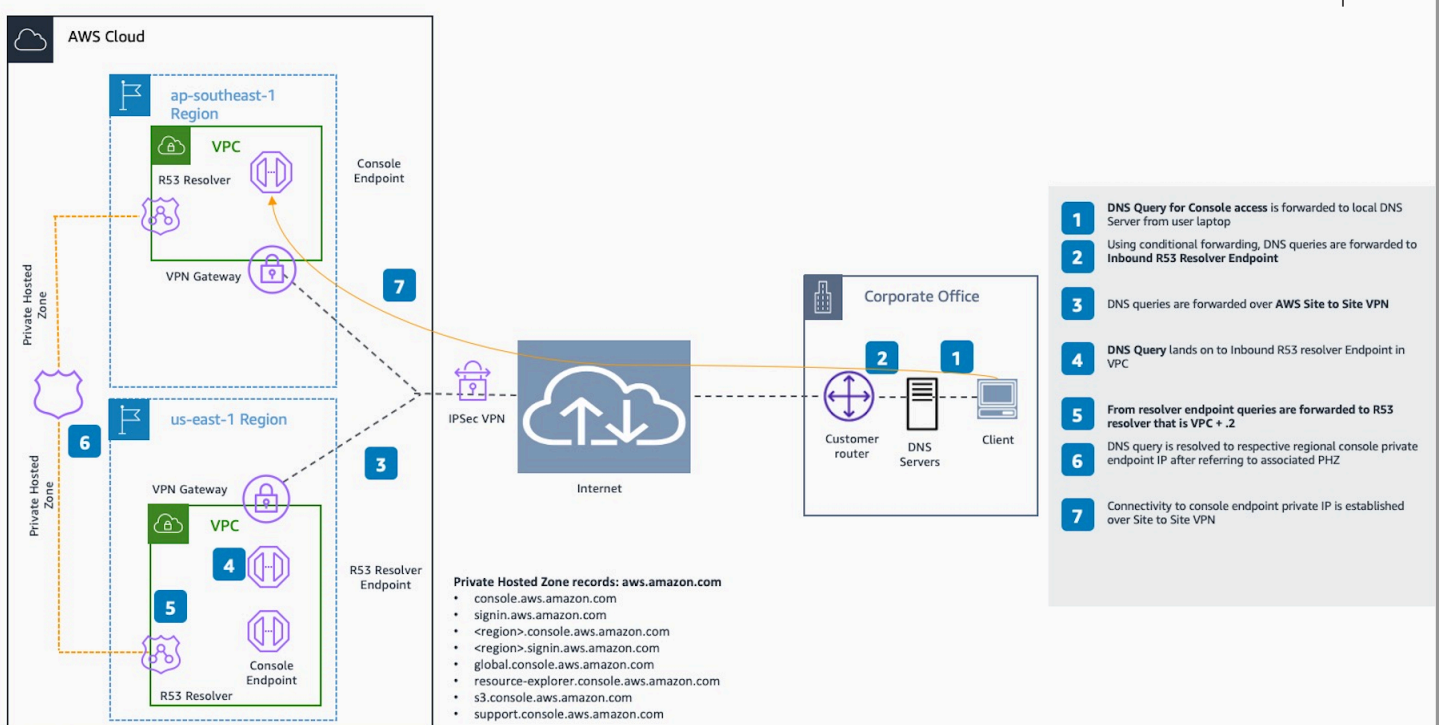
To access this account, sign in from a different network, or contact your administrator for more information.

Logout

Arsitektur referensi

Untuk terhubung secara pribadi ke Akses AWS Management Console 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 VPN AWS 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 AWS Management Console 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 AWS Management Console, mereka dirutekan ke IP AWS Management Console pribadi titik akhir Akses Pribadi.

Sebelum menyiapkan koneksi ke titik akhir Akses AWS Management Console Pribadi, selesaikan langkah-langkah prasyarat untuk menyiapkan titik akhir Akses AWS Management Console Pribadi

di semua Wilayah tempat Anda ingin mengakses AWS Management Console, serta di Wilayah AS Timur (Virginia N.), dan mengonfigurasi Zona Dihosting Pribadi.

Peluncuran AWS CloudShell di Toolbar Konsol

AWS CloudShell adalah shell terautentikasi berbasis peramban yang dapat Anda luncurkan langsung dari AWS Management Console pada Toolbar Konsol. Anda dapat menjalankan AWS CLI perintah pada layanan menggunakan shell pilihan Anda (Bash, PowerShell, atau Z shell).

Anda dapat meluncurkan CloudShell pada Console Toolbar menggunakan salah satu metode berikut:

- Pilih CloudShell ikon di kiri bawah konsol.
- Pilih CloudShell ikon pada bilah navigasi konsol konsol 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 sinkron dengan CloudShell Wilayah. Jika CloudShell tidak tersedia di Wilayah yang dipilih, maka CloudShell akan beroperasi di Wilayah terdekat.

Mendapatkan informasi penagihan

Jika Anda memiliki izin yang diperlukan, Anda dapat memperoleh informasi tentang biaya AWS Anda dari konsol.

Untuk mendapatkan informasi penagihan Anda

1. Di bilah navigasi, pilih nama akun Anda.
2. Pilih Dasbor Penagihan.
3. Gunakan dasbor AWS Billing and Cost Management untuk menemukan ringkasan dan rincian pengeluaran bulanan Anda. Untuk mempelajari selengkapnya, lihat [Panduan Pengguna AWS Billing](#).

Menggunakan Markdown di Konsol

Beberapa layanan di AWS Management Console, 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:

```
&nbsp;
&nbsp;
```

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, kelilingi 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 penurunan harga 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 AWS Management Console.

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 AWS Management Console](#)
- [Browser saya menampilkan kesalahan batas waktu saat menghubungkan ke AWS Management Console](#)
- [Saya ingin mengubah bahasa AWS Management Console 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 AWS Management Console. 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 AWS Management Console 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 AWS Management Console dengan browser lain yang didukung. Untuk informasi lebih lanjut, lihat [Blog AWS Berita](#).

Browser saya menampilkan kesalahan 'akses ditolak' saat menghubungkan ke AWS Management Console

Perubahan terbaru yang dilakukan pada konsol dapat memengaruhi akses Anda jika Anda menggunakan semua hal berikut:

- Browser dari dalam VPC.
- Titik akhir VPC.
- Kebijakan IAM yang berisi kunci kondisi `aws:SourceIp` global.

Di konsol, buka halaman kebijakan IAM. Kami menyarankan Anda meninjau kebijakan IAM yang berisi kunci kondisi `aws:SourceIp` global dan menambahkan `aws:SourceVpc` kunci.

Atau, Anda dapat mempertimbangkan orientasi ke fitur Akses AWS Management Console Pribadi untuk mengakses AWS Management Console melalui titik akhir VPC dan kondisi `aws:SourceVpc` penggunaan dalam kebijakan Anda. Untuk informasi selengkapnya, lihat [AWS Management Console Akses Pribadi](#).

Browser saya menampilkan kesalahan batas waktu saat menghubungkan ke AWS Management Console

Jika ada pemadaman layanan di default Anda Wilayah AWS, browser Anda mungkin menampilkan kesalahan 504 Gateway Timeout saat mencoba menyambung ke file. AWS Management Console Untuk masuk ke AWS Management Console 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-code.console.aws.amazon.com
```

Untuk informasi selengkapnya, lihat [titik akhir AWS Management Console layanan](#) di. Referensi Umum AWS

Untuk melihat status semua Layanan AWS, termasuk AWS Management Console, lihat [AWS Health Dashboard](#).

Saya ingin mengubah bahasa AWS Management Console 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 AWS Management Console, [navigasikan ke halaman Pengaturan Terpadu](#), lalu pilih bahasa untuk konsol.

Untuk informasi selengkapnya, lihat [Mengubah bahasa AWS Management Console](#).

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada Panduan AWS Management Console Memulai, mulai Maret 2021.

Perubahan	Deskripsi	Tanggal
Mengobrol dengan Amazon Q	Halaman pengaturan baru yang merinci bagaimana pengguna dapat mengajukan 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
Mengonfigurasi 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
AWS Console Home UI baru	AWS Console Home UI baru, yang mencakup widget untuk menampilkan informasi penggunaan penting dan pintasan ke layanan. AWS	25 Februari 2022

Perubahan	Deskripsi	Tanggal
	Untuk informasi selengkapnya, lihat Bekerja dengan widget .	
Mengubah bahasa Konsol	Pilih bahasa yang berbeda untuk AWS Management Console. Untuk informasi selengkapnya, lihat Mengubah bahasa AWS Management Console .	1 April 2021
Peluncuran CloudShell	Buka AWS CloudShell dari AWS Management Console dan jalankan perintah AWS CLI. Untuk informasi selengkapnya, lihat Peluncuran AWS CloudShell .	22 Maret 2021

AWSGlosarium

Untuk AWS terminologi terbaru, lihat [AWSglosarium di Referensi](#). Glosarium AWS

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