Panduan Implementasi

Ruang Tunggu Virtual di AWS

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

Ruang Tunggu Virtual di AWS: Panduan Implementasi

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 merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan properti dari masing-masing pemilik, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau tidak.

Table of Contents

Menyerap semburan besar lalu lintas ke situs web Anda dengan Ruang Tunggu Virtual di AWS

Tanggal publikasi: November 2021 (pembaruan terakhir: September 2024)

AWS Solusi Ruang Tunggu Virtual membantu mengontrol permintaan pengguna yang masuk ke situs web Anda selama ledakan lalu lintas yang besar. Ini menciptakan infrastruktur cloud yang dirancang untuk sementara menurunkan lalu lintas masuk ke situs web Anda, dan menyediakan opsi untuk menyesuaikan dan mengintegrasikan ruang tunggu virtual. Solusi ini dapat diintegrasikan dengan situs web baru atau yang sudah ada untuk skala mulus untuk menangani lonjakan lalu lintas yang tiba-tiba.

Contoh peristiwa skala besar yang dapat menghasilkan lonjakan lalu lintas situs web meliputi:

- Mulai penjualan tiket konser atau acara olahraga
- Fire sale atau penjualan eceran besar lainnya, seperti Black Friday
- Peluncuran produk baru dengan pengumuman pemasaran yang luas
- Akses ujian dan kehadiran kelas untuk pengujian dan pelajaran online
- Pelepasan slot janji medis
- Peluncuran direct-to-customer layanan baru yang membutuhkan pembuatan akun dan pembayaran

Solusinya bertindak sebagai area penahanan bagi pengunjung situs web Anda dan memungkinkan lalu lintas melewatinya ketika ada kapasitas yang cukup. Perangkat lunak klien yang digunakan oleh pengunjung dapat dikonfigurasi untuk secara transparan memungkinkan lalu lintas melalui ruang tunggu hingga situs web berada pada kapasitas maksimum; di mana ruang tunggu menahan pengunjung. Ketika situs web Anda memiliki kapasitas untuk lebih banyak lalu lintas, solusinya menghasilkan Token JSON Web (JWT) yang memungkinkan pengguna mengakses situs web. Misalnya, jika Anda memiliki acara yang berlangsung selama dua jam dan situs web Anda dapat memproses 50 pengguna per detik, tetapi Anda mengharapkan volume 250 per detik, maka Anda dapat menggunakan solusi ini untuk mengatur lalu lintas sambil memungkinkan pengguna untuk menjaga posisi mereka dalam antrian.

Solusi ini menyediakan fitur utama berikut:

- Antrian terstruktur pengguna ke situs web Anda

- Skalabilitas untuk mengontrol lalu lintas untuk ukuran acara yang sangat besar
- JSONpembuatan token web untuk memungkinkan masuk ke situs target
- Semua fungsi dikendalikan melalui REST APIs
- Otorisasi Turnkey API Gateway untuk solusi klien
- Integrasi mandiri atau gunakan dengan OpenID

Panduan implementasi ini menjelaskan pertimbangan arsitektur dan langkah-langkah konfigurasi untuk menerapkan Virtual Waiting Room AWS di Amazon Web Services (AWS) Cloud. Ini mencakup tautan ke AWS CloudFormationtemplat yang meluncurkan dan mengonfigurasi AWS layanan yang diperlukan untuk menerapkan solusi ini menggunakan praktik AWS terbaik untuk keamanan dan ketersediaan.

Panduan ini ditujukan untuk arsitek TI, pengembang, DevOps staf, analis data, dan profesional teknologi pemasaran yang memiliki pengalaman praktis dalam arsitektur Cloud. AWS

Biaya

Anda bertanggung jawab atas biaya AWS layanan yang digunakan saat menjalankan solusi ini. Pada revisi ini, biaya untuk menjalankan solusi ini dengan pengaturan default di Wilayah AS Timur (Virginia N.) adalah sekitar $10.00/hari per tumpukan ditambah biaya untuk permintaan API dan lalu lintas data relatif terhadap ukuran acara.

Biaya harian untuk mempertahankan solusi tanpa acara apa pun

AWS layanan	Permintaan/Waktu	Biaya [USD]
Amazon API Gateway	0	$0,00
Amazon CloudFront	0	$0,00
Amazon CloudWatch	0	$0,00
Amazon DynamoDB	0	$0,00
Amazon ElastiCache	Hitung jam node (Redis)	~$6,00
AWS Lambda	Tingkat gratis*	$0,00
AWS Secrets Manager	Tingkat gratis*	$0,00
Amazon Simple Storage Service (Amazon S3)	Tingkat gratis*	$0,00
Amazon Virtual Private Cloud (Amazon VPC)	Jam titik akhir VPC Jam gerbang NAT	~ $5,00
JUMLAH:		~$11,00

* Perkiraan biaya didasarkan pada lingkungan yang bersih. Jika Anda menggunakan layanan AWS ini di luar solusi ini, Anda dapat melebihi kuota tingkat gratis.

Tabel berikut menunjukkan perkiraan biaya untuk 50.000 pengguna dan ruang tunggu 100.000 pengguna dengan durasi acara berkisar 2-4 jam dengan 500 pengguna/detik masuk dan 1.000

pengguna/menit keluar. Harga dapat berubah sewaktu-waktu. Untuk detail selengkapnya, lihat halaman web harga untuk setiap AWS layanan yang digunakan dalam solusi ini.

Perkiraan biaya untuk 50.000 pengguna ruang tunggu selama 2 jam acara

AWS layanan	Dimensi	Biaya [USD]
Amazon API Gateway	Permintaan	$2,00
CloudFront	Permintaan, Bandwidth	$75.00
CloudWatch	Metrik, Alarm, Penyimpanan	$1,00
CloudWatch Acara Amazon	Peristiwa	$1,00
DynamoDB	Unit Baca/Tulis, Penyimpanan	$1,00
ElastiCache	Jam simpul	$8.00
Lambda	Permintaan, Waktu komputasi	$1,00
AWS Secrets Manager	Rahasia, Permintaan	$1,00
Amazon S3	Permintaan, Penyimpanan	$1,00
Amazon VPC	Transfer data, Waktu titik akhir	$2,00
TOTAL		$94.00

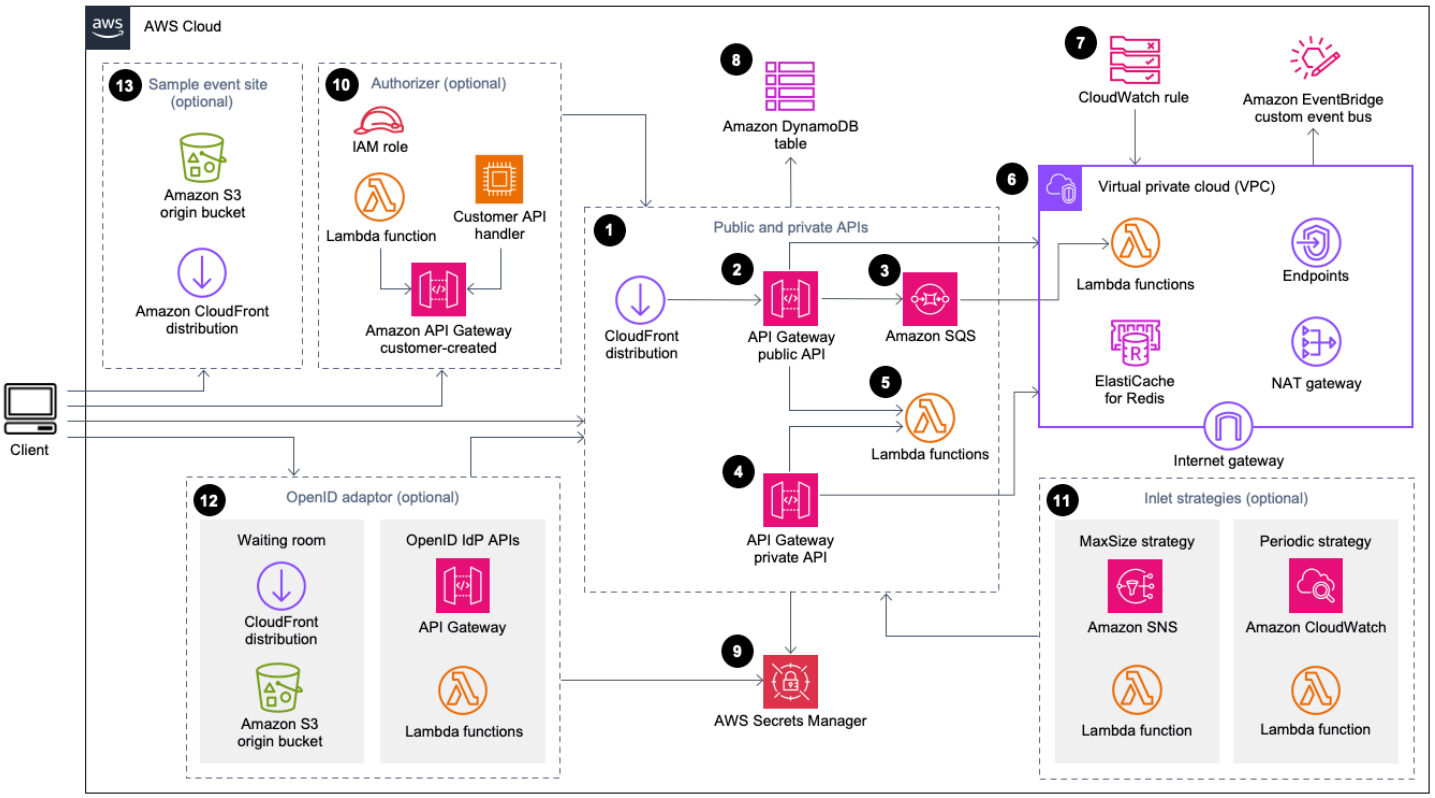
Perkiraan biaya untuk 100.000 pengguna ruang tunggu selama 2 jam acara

AWS layanan	Dimensi	Biaya [USD]
Amazon API Gateway	Permintaan	$4,00

CloudFront	Permintaan, Bandwidth	$296.00
CloudWatch	Metrik, Alarm, Penyimpanan	$1,00
CloudWatch Acara	Peristiwa	$1,00
DynamoDB	Unit Baca/Tulis, Penyimpanan	$4,00
ElastiCache	Jam simpul	$32,00
Lambda	Permintaan, Waktu komputasi	$1,00
AWS Secrets Manager	Rahasia, Permintaan	$1,00
Amazon Simple Queue Service (Amazon SQS)	Permintaan	$1,00
Amazon S3	Permintaan, Penyimpanan	$1,00
Amazon VPC	Transfer data, Waktu titik akhir	$6,00
TOTAL		$348.00

Gambaran umum arsitektur

Menerapkan solusi ini dengan templat yang diperlukan dan opsional, menggunakan parameter default, membangun lingkungan berikut di AWS Cloud.



Ruang Tunggu Virtual pada AWS arsitektur

AWS CloudFormation Template menyebarkan infrastruktur berikut:

1. CloudFrontDistribusi Amazon untuk menyampaikan API panggilan publik untuk klien.
2. APISumber daya publik Amazon API Gateway untuk memproses permintaan antrian dari ruang tunggu virtual, melacak posisi antrian, dan mendukung validasi token yang memungkinkan akses ke situs web target.
3. Antrian Amazon Simple Queue Service (AmazonSQS) untuk mengatur lalu lintas ke AWS Lambdafungsi yang memproses pesan antrian. Alih-alih menjalankan fungsi Lambda untuk setiap permintaan, antrian SQS akan mengumpulkan semburan permintaan yang masuk.
4. APIGateway API sumber daya pribadi untuk mendukung fungsi administrasi.
5. Lambda berfungsi untuk memvalidasi dan memproses API permintaan publik dan pribadi, dan mengembalikan tanggapan yang sesuai.

6. Amazon Virtual Private Cloud (VPC) untuk meng-host fungsi Lambda yang berinteraksi langsung dengan cluster Elasticache (Redis). OSS VPCendpoint memungkinkan fungsi Lambda untuk berkomunikasi dengan layanan dalam solusi. VPC Selain itu, NAT gateway memungkinkan fungsi Lambda VPC untuk menghubungkan CloudFront titik akhir dan membatalkan cache sesuai kebutuhan.
7. CloudWatchAturan Amazon untuk menjalankan fungsi Lambda yang berfungsi dengan bus EventBridgeAmazon khusus untuk menyiarkan pembaruan status secara berkala.
8. Tabel Amazon DynamoDB untuk menyimpan token, posisi antrian, dan menyajikan data penghitung.
9. AWS Secrets Manager untuk menyimpan kunci untuk operasi token dan data sensitif lainnya.
10. (Opsional) Komponen Authorizer yang terdiri dari peran AWS Identity and Access Management(IAM) dan fungsi otorisasi Lambda untuk digunakan dengan Gateway. API
11. (Opsional) Amazon Simple Notification Service (AmazonSNS), CloudWatch, dan Lambda berfungsi untuk mendukung dua strategi inlet.
12. (Opsional) Komponen adaptor OpenID dengan fungsi API Gateway dan Lambda untuk memungkinkan penyedia OpenID mengautentikasi pengguna ke situs web Anda. CloudFront distribusi dengan bucket Amazon Simple Storage Service (Amazon S3) untuk halaman ruang tunggu komponen ini.
13. CloudFront Distribusi (Opsional) dengan bucket asal Amazon S3 untuk contoh aplikasi web ruang tunggu.

Bagaimana solusinya bekerja

Bagian ini menjelaskan langkah-langkah dalam alur kerja Ruang Tunggu AWS Virtual pada tingkat tinggi. Lihat Panduan Pengembang GitHub untuk detail tentang membangun, menyesuaikan, dan mengintegrasikan ruang tunggu untuk situs web Anda.

Ruang tunggu publik API dapat ditempatkan di belakang keamanan perimeter situs Anda atau dapat tersedia tanpa otorisasi apa pun. Bergantung pada pendekatan yang Anda gunakan untuk mengintegrasikan ruang tunggu dengan situs web, pengguna mungkin diminta untuk terlebih dahulu mengautentikasi ke situs web sebelum diizinkan untuk menavigasi ke ruang tunggu dan mendapatkan posisi dalam antrian.

Perangkat lunak klien harus memiliki ID Acara untuk memasuki ruang tunggu dan membuat permintaan lainnya. ID Acara adalah ID unik yang diperlukan untuk sebagian besar permintaan terhadap publik dan pribadiAPIs. ID Peristiwa diatur selama instalasi API tumpukan inti. Selama operasi, ID Acara dapat diberikan sebagai URL parameter atau cookie melalui halaman ruang tunggu; itu dapat disediakan sebagai bagian dari klaim token otentikasi atau dapat didistribusikan ke klien melalui jalur data yang berbeda.

Ada kasus di mana klien membutuhkan ID Acara dan ID Permintaan untuk melakukan API panggilan tertentu. ID Permintaan adalah ID unik yang dikeluarkan dari ruang tunggu yang mewakili klien tertentu dalam antrean.

Langkah-langkah berikut menjelaskan alur API permintaan untuk entri antrian, menunggu antrian berkembang, dan keluar dari ruang tunggu dengan token akses untuk situs web.

Pengguna memasuki ruang tunggu:

1. Pengguna disajikan dengan layar atau halaman yang mewakili titik masuk ruang tunggu. Mereka memilih untuk memasuki antrian dan perangkat lunak klien (browser, seluler, perangkat) memanggil `assign_queue_num` publik API untuk meminta posisi antrian.
2. APIPermintaan segera dikirim ke SQS antrian Amazon oleh API Gateway.
3. `assign_queue_num`APIPanggilan kembali ketika permintaan ditempatkan ke dalam antrian. Klien menerima ID Permintaan unik yang dapat digunakan nanti untuk mengambil posisi antrian, waktu permintaan, dan token akses.
4. Fungsi `AssignQueueNum` Lambda menerima batch hingga sepuluh permintaan dari antrian. SQS Layanan Lambda menggemari pemanggilan untuk memproses beberapa batch permintaan.

5. Fungsi `AssignQueueNum` Lambda memvalidasi setiap pesan dalam batch, menambah penghitung antrian di Elasticache (RedisOSS), dan menyimpan setiap permintaan di Elasticache (Redis) dengan posisi antrian yang terkait. OSS
6. Setiap pesan dihapus karena berhasil diproses. Pesan yang terlibat dalam kondisi kesalahan diproses ulang sekali dalam batch berikutnya. Setelah kegagalan kedua, mereka dikirim ke yang dead-letter-queue terhubung ke CloudWatchalarm.
7. Klien dapat memulai polling `queue_num` API setelah menerima ID Permintaan dari `assign_queue_num` panggilan. Klien mengirimkan ID Peristiwa dan ID Permintaan ke `queue_num` API dan menerima posisi antrian numerik atau respons yang menunjukkan permintaan belum diproses. Klien mungkin perlu melakukan panggilan ini lebih dari sekali selama acara besar. Fungsi `GetQueueNum` Lambda dipanggil oleh API Gateway dan mengembalikan posisi numerik klien dalam antrian dari DynamoDB.

Pengguna menunggu di ruang tunggu:

8. Setelah klien memiliki posisi dalam antrian, ia dapat mulai polling `serving_num` API pada interval reguler. `serving_num`APIIni dipanggil dengan ID Peristiwa dan mengembalikan posisi penyajian antrian saat ini. Respons dari klien `serving_num` API memberi tahu klien kapan mereka dapat berpindah dari ruang tunggu ke situs target yang sebenarnya di mana transaksi akhir dapat terjadi. Fungsi `GetServingNum` Lambda mengembalikan posisi servis saat ini dari ruang tunggu.
9. Ketika posisi servis sama dengan atau lebih besar dari posisi antrian (permintaan) klien, klien dapat meminta Token JSON Web (JWT) dari publikAPI. Token dapat digunakan dengan situs target untuk menyelesaikan transaksi. Disebut dengan ID Acara dan ID Permintaan. `generate_token` API APIGateway memanggil fungsi `GenerateToken` Lambda dengan parameter.
10. Fungsi `GenerateToken` Lambda memvalidasi permintaan dan memeriksa apakah token ini telah dibuat sebelumnya. Fungsi Lambda menanyakan tabel DynamoDB untuk token yang cocok. Jika ditemukan, token itu dikembalikan ke pemanggil dan tidak dibuat ulang. Proses ini mencegah satu ID Permintaan digunakan untuk menghasilkan beberapa token berbeda dengan waktu kedaluwarsa baru.
11. Jika token tidak ditemukan di DynamoDB, fungsi Lambda mengambil kunci untuk membuat token dan menyimpan token di DynamoDB dengan ID Peristiwa dan ID Permintaan klien. Fungsi Lambda menulis sebuah peristiwa EventBridge untuk memberi sinyal bahwa token baru telah dihasilkan. Fungsi Lambda menambah penghitung Elasticache (RedisOSS) yang melacak jumlah token yang dihasilkan untuk acara tersebut.

12. Jika `queue_pos_expiry` dihidupkan, klien dapat menanyakan sisa waktu sebelum kedaluwarsa dengan memanggil fungsi Lambda `queue_pos_expiry` API yang memanggil fungsi LambdaGetQueuePositionExpiryTime.

Pengguna meninggalkan ruang tunggu:

13. Ketika klien menerima tokennya, ia memasuki situs target untuk memulai transaksinya. Bergantung pada bagaimana infrastruktur Anda mendukung integrasiJWT, klien mungkin perlu menyajikan token di header permintaan, cookie, atau cara lain. Authorizer untuk API Gateway dapat digunakan untuk memvalidasi token yang disertakan dalam permintaan klien. Pustaka komersial atau sumber terbuka apa pun untuk memvalidasi dan mengelola JWTs dapat digunakan dengan Ruang Tunggu Virtual pada token. AWS Jika token valid, klien diizinkan untuk melanjutkan transaksi mereka.
14. Setelah klien menyelesaikan transaksi mereka, private API dipanggil untuk memperbarui status token klien dan diselesaikan di DynamoDB.

Kedaluwarsa posisi antrian:

15. Ketika fitur ini diaktifkan, ID Permintaan yang sesuai dengan posisi antrian tertentu memenuhi syarat untuk menghasilkan token hanya untuk interval waktu tertentu.

Penghitung penayangan kenaikan pada posisi antrian kedaluwarsa:

16. Ketika fitur ini diaktifkan, penghitung penayangan secara otomatis bertambah berdasarkan posisi antrian kedaluwarsa yang tidak dapat menghasilkan token.

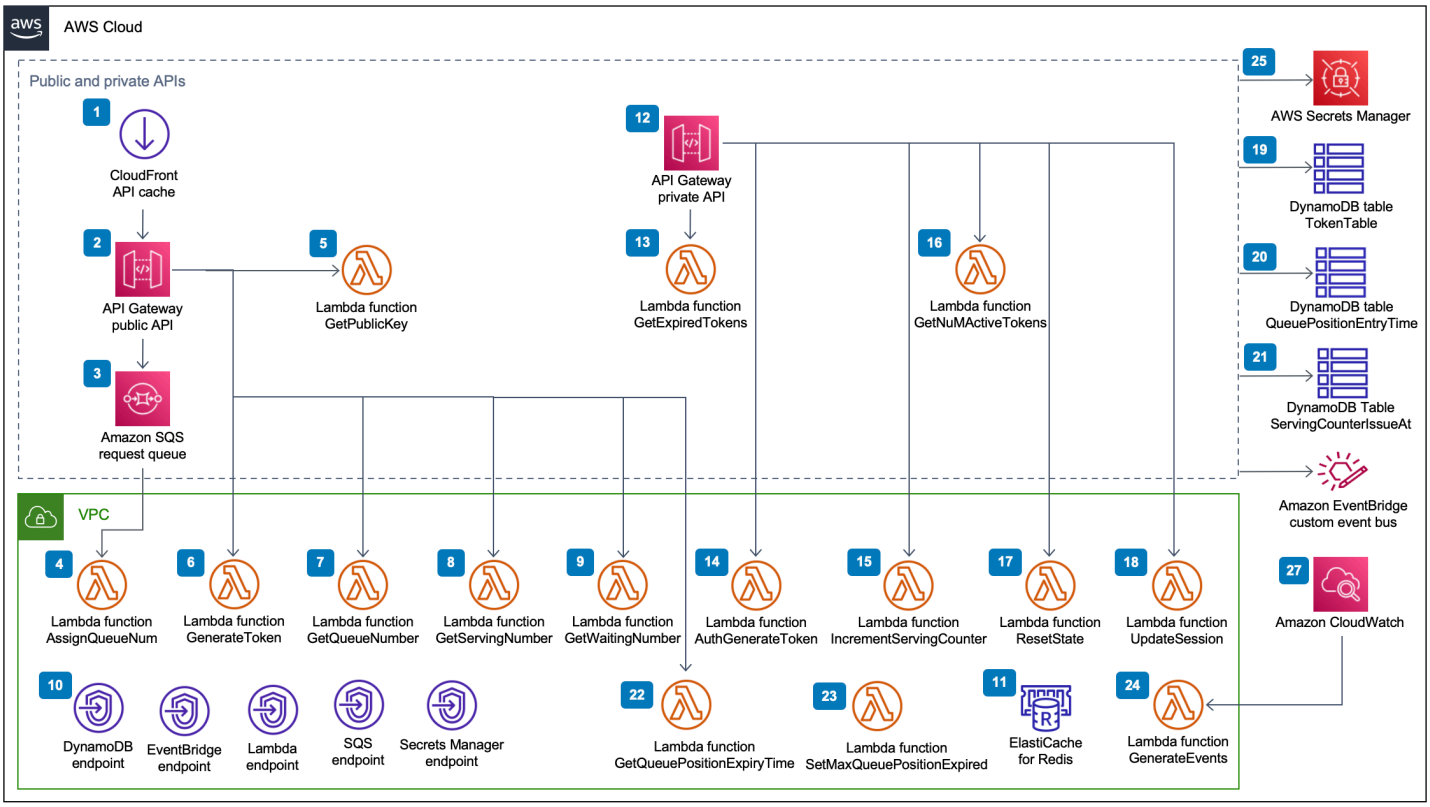
Komponen solusi

Ruang tunggu publik dan pribadi APIs

Ruang Tunggu Virtual pada tujuan utama AWS solusi adalah untuk mengontrol pembuatan Token JSON Web (JWT) untuk klien dengan cara yang terkontrol untuk menghindari ledakan pengguna baru yang mungkin membanjiri situs web tujuan. JWTsDapat digunakan untuk perlindungan situs, mencegah akses ke halaman web sampai token ruang tunggu diperoleh, dan juga untuk otorisasi API akses.

Template inti menginstal publik API dan pribadi (IAM-authorized) yang API digunakan untuk sebagian besar Ruang Tunggu Virtual pada AWS operasi. Publik API dikonfigurasi dengan CloudFront distribusi dengan beberapa kebijakan caching berdasarkan API jalur. Tabel DynamoDB EventBridge dan bus acara dibuat. Template menambahkan yang baru VPC dengan dua Availability Zones (AZs), cluster Elasticache (RedisOSS) di keduanyaAZs, dan beberapa fungsi Lambda. Fungsi Lambda yang berinteraksi dengan Elasticache (RedisOSS) memiliki antarmuka jaringan di dalam dan VPC semua fungsi Lambda lainnya memiliki konektivitas jaringan default. Inti APIs adalah lapisan terendah interaksi dengan solusi. Fungsi Lambda lainnya, instans Amazon Elastic Compute Cloud (AmazonEC2), dan container dapat bertindak sebagai ekstensi dan memanggil inti APIs untuk membangun ruang tunggu, mengontrol lalu lintas masuk, dan bereaksi terhadap peristiwa yang dihasilkan dari solusi.

Selain itu, tumpukan inti membuat alarm untuk semua kesalahan fungsi Lambda dan kondisi throttle, serta alarm untuk setiap penerapan API Gateway untuk kode status 4XX dan 5XX.



Ruang Tunggu Virtual pada APIs komponen AWS Publik dan Pribadi

1. CloudFront distribusi memberikan API panggilan publik untuk klien dan hasil cache jika sesuai.
2. Permintaan antrian API proses publik Amazon API Gateway dari ruang tunggu virtual, lacak posisi antrian, dan dukung validasi token yang memungkinkan akses ke situs web target.
3. SQSantrian mengatur lalu lintas ke AWS Lambda fungsi yang memproses pesan antrian.
4. Fungsi `AssignQueueNum` Lambda memvalidasi setiap pesan dalam batch yang diterima, menambah penghitung antrian di Elasticache (RedisOSS), dan menyimpan setiap permintaan di Elasticache (Redis) dengan posisi antrian yang terkait. OSS
5. Fungsi `GetPublicKey` Lambda mengambil nilai kunci publik dari Secrets Manager.
6. Fungsi `GenerateToken` Lambda menghasilkan permintaan yang JWT valid yang telah diizinkan untuk menyelesaikan transaksinya di situs target. Ini menulis acara ke bus acara khusus ruang tunggu bahwa token telah dibuat. Jika token sebelumnya telah dibuat untuk permintaan ini, tidak ada token baru yang dihasilkan.
7. Fungsi `GetQueueNumber` Lambda mengambil dan mengembalikan posisi numerik klien dalam antrian dari Elasticache (Redis). OSS

8. Fungsi `GetServingNumber` Lambda mengambil dan mengembalikan nomor yang saat ini sedang dilayani oleh ruang tunggu dari Elasticache (Redis). OSS
9. Fungsi `GetWaitingNum` Lambda mengembalikan nomor yang saat ini mengantri di ruang tunggu dan belum dikeluarkan token.
10. VPCendpoint memungkinkan fungsi Lambda untuk berkomunikasi dengan layanan dalam solusi. VPC
11. Cluster Elasticache (RedisOSS) menyimpan semua permintaan untuk memasuki ruang tunggu dengan ID Peristiwa yang valid. Ini juga menyimpan beberapa penghitung seperti jumlah permintaan yang diantrekan, jumlah yang saat ini dilayani, jumlah token yang dihasilkan, jumlah sesi yang diselesaikan, dan jumlah sesi yang ditinggalkan.
12. APIGateway API sumber daya pribadi untuk mendukung fungsi administratif. Pribadi APIs AWS IAM diautentikasi.
13. Fungsi `GetExpiredTokens` Lambda mengembalikan daftar permintaan dengan token IDs kedaluwarsa.
14. Fungsi `AuthGenerateToken` Lambda menghasilkan token untuk permintaan valid yang telah diizinkan untuk menyelesaikan transaksinya di situs target. Penerbit dan masa berlaku token yang awalnya ditetapkan selama penerapan tumpukan inti dapat diganti. Ini menulis acara ke bus acara khusus ruang tunggu bahwa token telah dibuat. Jika token sebelumnya telah dibuat untuk permintaan ini, tidak ada token baru yang dihasilkan.
15. Fungsi `IncrementServingCounter` Lambda meningkatkan penghitung penyajian ruang tunggu yang disimpan di Elasticache (RedisOSS) dengan kenaikan nilai.
16. Fungsi `GetNumActiveTokens` Lambda menanyakan DynamoDB untuk jumlah token yang belum kedaluwarsa, belum digunakan untuk menyelesaikan transaksinya, dan belum ditandai ditinggalkan.
17. Fungsi `ResetState` Lambda me-reset semua counter yang disimpan di Elasticache (Redis). OSS Ini juga menghapus dan membuat ulang tabel`TokenTable`,`QueuePositionEntryTime`, dan DynamoDB`ServingCounterIssuedAt`. Selain itu, ia melakukan pembatalan CloudFront cache.
18. Fungsi `UpdateSession` Lambda memperbarui status sesi (token) yang disimpan dalam tabel DynamoDB`TokenTable`. Status sesi dilambangkan dengan bilangan bulat. Sesi diatur ke status `1` menunjukkan selesai, dan `-1` menunjukkan ditinggalkan. Ini menulis acara ke bus acara khusus ruang tunggu bahwa sesi telah diperbarui.
19. Tabel `TokenTable` DynamoDB menyimpan data token.
20. Tabel `QueuePositionEntryTime` DynamoDB menyimpan data posisi antrian dan waktu masuk.
21. Tabel `ServingCounterIssuedAt` DynamoDB menyimpan pembaruan ke konter penyajian.

22 Fungsi `GetQueuePositionExpireTime` Lambda dipanggil ketika klien meminta waktu kedaluwarsa posisi antrian yang tersisa.

23 Fungsi `SetMaxQueuePositionExpired` Lambda menetapkan posisi antrian maksimum yang telah kedaluwarsa sesuai dengan nilai tabel. `ServingCounterIssuedAt` Ini berjalan setiap menit jika `IncrSvcOnQueuePositionExpiry` parameter disetel ke `true` selama penyebaran tumpukan inti.

24 Fungsi `GenerateEvents` Lambda menulis berbagai metrik ruang tunggu ke bus acara khusus ruang tunggu. Ini dijalankan setiap menit jika parameter Aktifkan Pembuatan Acara disetel ke `true` selama penerapan tumpukan inti.

25 AWS Secrets Manager menyimpan kunci untuk operasi token dan data sensitif lainnya.

26 Bus acara EventBridge khusus Amazon menerima acara setiap kali token dibuat dan sesi diperbarui di tabel `TokenTable` DynamoDB. Itu juga menerima acara ketika konter penyajian dipindahkan di `SetMaxQueuePositionExpired` Lambda. Itu ditulis dengan berbagai metrik ruang tunggu, jika diaktifkan selama penerapan tumpukan inti.

27 Aturan CloudWatch peristiwa Amazon dibuat jika parameter Aktifkan Pembuatan Acara disetel ke true selama penerapan tumpukan inti. Aturan acara ini memulai fungsi `GenerateEvents` Lambda setiap menit.

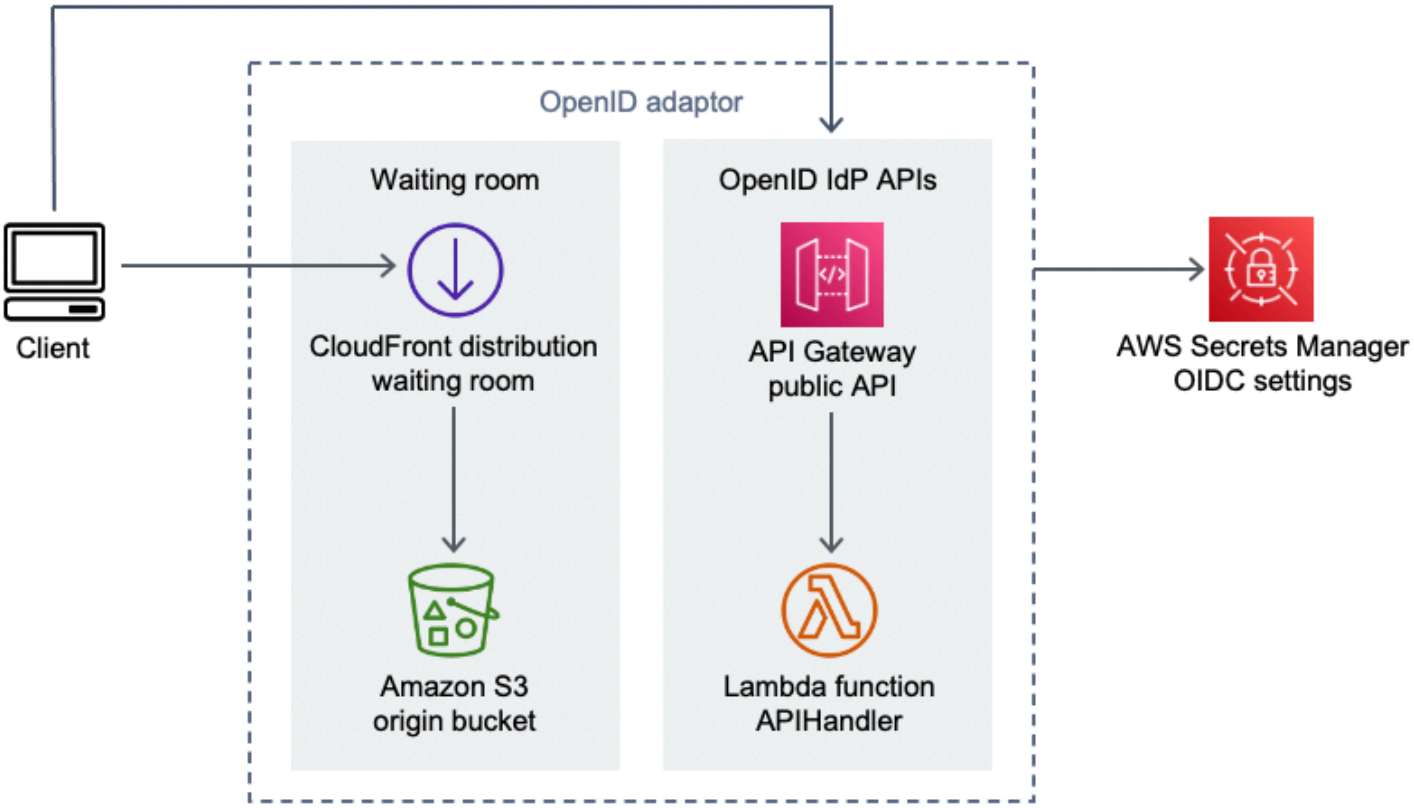
Pengotorisasi

Solusinya mencakup tumpukan otorisasi API Gateway Lambda. Tumpukan terdiri dari satu IAM peran dan fungsi Lambda. Fungsi `APIGatewayAuthorizer` Lambda adalah otorisasi untuk API Gateway yang dapat memvalidasi tanda tangan dan klaim token yang dikeluarkan oleh Ruang Tunggu Virtual pada. AWS API Fungsi Lambda yang disertakan dengan tumpukan dapat digunakan untuk melindungi cloud APIs sampai pengguna telah maju melalui ruang tunggu dan menerima token akses. Authorizer secara otomatis mengambil dan menyimpan kunci publik dan konfigurasi dari inti API untuk verifikasi token. Ini dapat digunakan tanpa modifikasi dan dapat diinstal di AWS Wilayah mana pun yang mendukung AWS Lambda.

Adaptor OpenID

Tumpukan adaptor OpenID menyebarkan fungsi Gateway API dan Lambda yang bertindak sebagai penyedia identitas OpenID. Adaptor OpenID menyediakan seperangkat OIDC -kompatibel APIs yang dapat digunakan dengan perangkat lunak hosting web yang ada yang mendukung penyedia OIDC identitas, seperti AWS Elastic Load Balancers, WordPress, atau sebagai penyedia identitas federasi

untuk Amazon Cognito atau layanan serupa. Adaptor memungkinkan pelanggan untuk menggunakan ruang tunggu dalam aliran AuthN/Authz saat menggunakan perangkat lunak hosting off-the-shelf web dengan opsi integrasi terbatas. Tumpukan juga menginstal CloudFront distribusi dengan satu bucket Amazon S3 sebagai asal dan bucket S3 lainnya untuk permintaan logging. Adaptor OpenID menyajikan contoh halaman ruang tunggu, mirip dengan yang disediakan di tumpukan ruang tunggu sampel, tetapi dirancang untuk aliran otentikasi OpenID. Proses menjadi otentikasi melibatkan mendapatkan posisi dalam antrian ruang tunggu dan menunggu sampai posisi servis sama atau lebih besar dari posisi antrian klien. Halaman ruang tunggu OpenID dialihkan kembali ke situs target, yang menggunakan OpenID API untuk menyelesaikan akuisisi token dan konfigurasi sesi untuk klien. APITitik akhir solusi ini memetakan langsung ke spesifikasi aliran name-for-name OpenID Connect 1.0 resmi,. Lihat [OpenID Connect Core 1.0 Otentikasi] untuk detailnya.



Ruang Tunggu Virtual pada komponen AWS adaptor OpenID

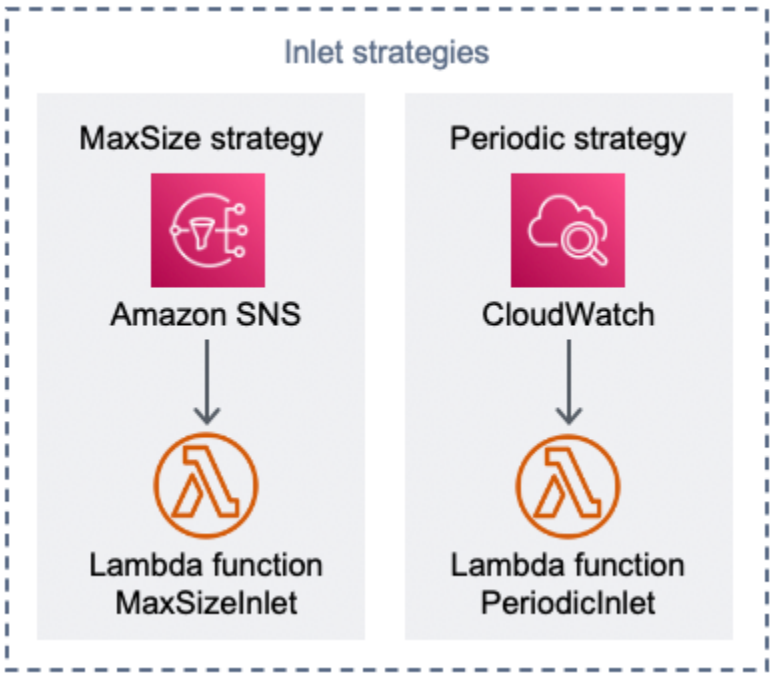
1. CloudFront distribusi menyajikan konten bucket S3 kepada pengguna.
2. Bucket S3 menampung contoh halaman ruang tunggu.
3. Amazon API Gateway API menyediakan seperangkat OIDC -kompatibel APIs yang dapat digunakan dengan perangkat lunak hosting web yang ada yang mendukung fungsi OIDC otorisasi Lambda penyedia identitas.

4. Fungsi `APIHandler` Lambda menangani permintaan untuk semua jalur sumber daya API Gateway. Fungsi Python yang berbeda dalam modul yang sama dipetakan ke setiap jalur. API Misalnya, jalur `/authorize` sumber daya di API Gateway dipanggil `authorize()` dalam Fungsi Lambda.
5. OIDCpengaturan disimpan di Secrets Manager.

Contoh strategi saluran masuk

Strategi inlet menentukan kapan penghitung penyajian solusi harus bergerak maju untuk mengakomodasi lebih banyak pengguna di situs target. Untuk informasi konseptual lebih lanjut tentang strategi saluran masuk ruang tunggu, lihat Pertimbangan desain.

Ada dua strategi inlet sampel yang disediakan oleh solusi: MaxSizedan Periodik.



Ruang Tunggu Virtual pada AWS komponen strategi Inlet

Opsi strategi inlet Ukuran Maks:

1. Klien mengeluarkan SNS notifikasi Amazon yang memanggil fungsi `MaxSizeInlet` Lambda untuk meningkatkan penghitung penayangan berdasarkan payload pesan.
2. Fungsi `MaxSizeInlet` Lambda mengharapkan untuk menerima pesan yang digunakannya menentukan berapa banyak untuk meningkatkan penghitung penyajian.

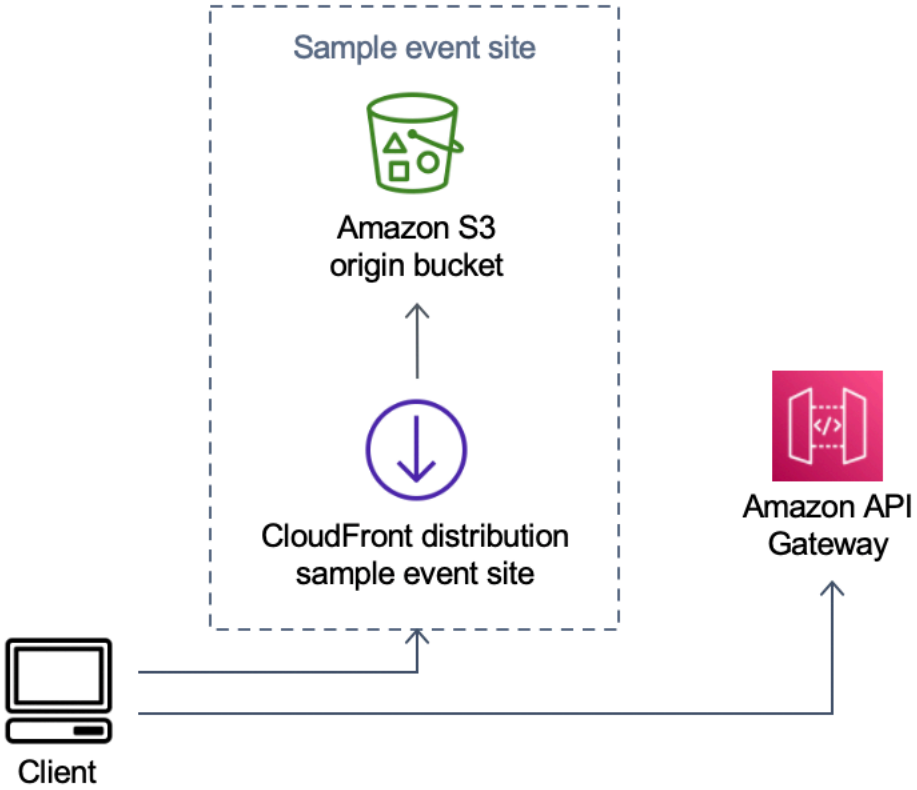
Opsi strategi saluran masuk berkala:

3. CloudWatch Aturan memanggil fungsi Lambda setiap menit untuk meningkatkan penghitung porsi dengan jumlah tetap.
4. Fungsi `PeriodicInlet` Lambda menambah penghitung penyajian dengan ukuran yang diberikan jika waktu antara waktu mulai dan akhir yang disediakan. Secara opsional, ia memeriksa CloudWatch alarm dan, jika alarm dalam `OK` keadaan, melakukan kenaikan, jika tidak, lewati saja.

Contoh ruang tunggu

Ruang tunggu sampel terintegrasi dengan publik dan swasta APIs selain otorisasi khusus untuk menunjukkan solusi ruang end-to-end tunggu minimal. Halaman web utama disimpan dalam ember S3 dan digunakan sebagai asal. CloudFront Dibutuhkan pengguna melalui langkah-langkah berikut:

1. Antrean di ruang tunggu untuk masuk ke situs.
2. Dapatkan posisi klien dalam antrean.
3. Dapatkan posisi melayani ruang tunggu.
4. Dapatkan set token setelah posisi servis sama atau lebih besar dengan posisi klien.
5. Gunakan token untuk memanggil yang API dilindungi oleh otorisasi Lambda.



Ruang Tunggu Virtual pada AWS Contoh komponen situs acara

1. Bucket S3 menampung konten sampel untuk ruang tunggu dan panel kontrol.
2. CloudFront distribusi menyajikan konten bucket S3 kepada pengguna.
3. Contoh penerapan API Gateway dengan jalur sumber daya seperti belanja seperti dan. `/search` `/checkout` APIIni diinstal oleh tumpukan dan dikonfigurasi dengan otorisasi token. Ini dimaksudkan sebagai contoh cara sederhana untuk melindungi API dengan ruang tunggu. Permintaan yang menyajikan token yang valid diteruskan ke Lambda, jika tidak, kesalahan akan dikembalikan. Tidak ada fungsionalitas API selain respons dari fungsi Lambda yang terpasang.

Keamanan

Ketika Anda membangun sistem di atas AWS infrastruktur, tanggung jawab keamanan dibagi antara Anda dan AWS. Model bersama ini mengurangi beban operasional Anda karena AWS mengoperasikan, mengelola, dan mengontrol komponen termasuk sistem operasi host, lapisan virtualisasi, dan keamanan fisik fasilitas tempat layanan beroperasi. Untuk informasi selengkapnya tentang AWS keamanan, kunjungi AWS Cloud Security.

Elasticache (RedisOSS) ditugaskan antarmuka jaringan di dalam pribadi. VPC Fungsi Lambda yang berinteraksi dengan Elasticache (RedisOSS) juga ditetapkan antarmuka jaringan dalam file. VPC Semua sumber daya lainnya memiliki konektivitas jaringan di ruang AWS jaringan bersama. Fungsi Lambda dengan VPC antarmuka yang berinteraksi dengan AWS layanan lain menggunakan VPC titik akhir untuk terhubung ke layanan ini.

Kunci publik dan pribadi yang digunakan untuk membuat dan memvalidasi token JSON web dihasilkan pada waktu penerapan dan disimpan di Secrets Manager. Kata sandi yang digunakan untuk terhubung ke Elasticache (RedisOSS) juga dihasilkan pada waktu penerapan dan disimpan di Secrets Manager. Kunci pribadi dan kata sandi Elasticache (RedisOSS) tidak dapat diakses melalui solusi apa pun. API

Publik API harus diakses melalui CloudFront APISolusinya menghasilkan kunci untuk API Gateway, yang digunakan sebagai nilai header khusus,`x-api-key`, di CloudFront. CloudFront menyertakan header ini saat membuat permintaan asal. Untuk detail tambahan, lihat Menambahkan header khusus ke permintaan asal di Panduan CloudFront Pengembang Amazon.

Privat APIs dikonfigurasi untuk memerlukan AWS IAM otorisasi untuk pemanggilan. Solusinya membuat grup `ProtectedAPIGroup` IAM pengguna dengan izin yang sesuai untuk memanggil privat. APIs IAMPengguna yang ditambahkan ke grup ini diberi wewenang untuk memanggil pribadiAPIs.

IAMkebijakan yang digunakan dalam peran dan izin yang dilampirkan ke berbagai sumber daya yang dibuat oleh solusi hanya memberikan izin yang diperlukan untuk melakukan tugas yang diperlukan.

Untuk sumber daya seperti bucket S3, SQS antrian, dan SNS topik yang dihasilkan oleh solusi, enkripsi saat istirahat dan selama transit diaktifkan sedapat mungkin.

Pemantauan

APITumpukan inti mencakup beberapa CloudWatch alarm yang dapat dipantau untuk mendeteksi masalah saat solusinya beroperasi. Tumpukan membuat alarm untuk kesalahan fungsi Lambda dan kondisi throttle, dan mengubah status alarm dari `OK` `ALARM` jika terjadi kesalahan atau kondisi throttle dalam periode satu menit.

Tumpukan juga membuat alarm untuk setiap penerapan API Gateway untuk kode status 4XX dan 5XX. Alarm berubah status dari `OK` menjadi `ALARM` jika kode status 4XX atau 5XX dikembalikan dari API dalam jangka waktu satu menit.

Alarm ini kembali ke `OK` keadaan setelah satu menit tidak ada kesalahan atau throttle.

IAMperan

AWS Identity and Access Management (IAM) peran memungkinkan pelanggan untuk menetapkan kebijakan akses terperinci dan izin untuk layanan dan pengguna di Cloud. AWS Solusi ini menciptakan IAM peran yang memberikan akses AWS Lambda fungsi solusi untuk membuat sumber daya Regional.

Amazon CloudFront

`virtual-waiting-room-on-aws.template` CloudFormation Template, yang menciptakan inti publik dan pribadi APIs ruang tunggu, juga menyebarkan CloudFront distribusi untuk publikAPI. CloudFront menyimpan respons dari publikAPI, sehingga mengurangi beban pada API Gateway dan fungsi Lambda yang melakukan pekerjaan.

Solusi ini juga memiliki contoh template ruang tunggu opsional yang menyebarkan aplikasi web sederhana yang dihosting di bucket Amazon Simple Storage Service (Amazon S3). Untuk membantu mengurangi latensi dan meningkatkan keamanan, CloudFront distribusi Amazon diterapkan dengan identitas akses asal, yaitu CloudFront pengguna yang menyediakan akses publik ke konten bucket situs web solusi. Untuk informasi selengkapnya, lihat Membatasi Akses ke Konten Amazon S3 dengan Menggunakan Identitas Akses Asal di Panduan Pengembang CloudFront Amazon.

Grup keamanan

Grup VPC keamanan yang dibuat dalam solusi ini dirancang untuk mengontrol dan mengisolasi lalu lintas jaringan ke Elasticache (Redis). OSS Lambda yang perlu berkomunikasi dengan Elasticache

(RedisOSS) ditempatkan di Grup Keamanan yang sama dengan Elasticache (Redis). OSS Kami menyarankan Anda meninjau grup keamanan dan membatasi akses lebih lanjut sesuai kebutuhan setelah penerapan aktif dan berjalan.

Pertimbangan desain

Opsi deployment

Jika ini adalah pertama kalinya menginstal, atau Anda tidak yakin apa yang harus diinstal, gunakan CloudFormation template `virtual-waiting-room-on-aws-getting-started.template` bersarang, yang menginstal inti, otorisasi, dan contoh template ruang tunggu. Ini memberi Anda ruang tunggu minimal dengan aliran sederhana.

Protokol yang didukung

AWS Solusi Ruang Tunggu Virtual dapat diintegrasikan dengan yang berikut:

- JSONPustaka dan alat verifikasi Token Web
- Penerapan API Gateway yang ada
- RESTAPIklien
- Klien dan penyedia OpenID

Strategi inlet ruang tunggu

Strategi inlet merangkum logika dan data yang diperlukan untuk memindahkan klien dari ruang tunggu ke situs web. Strategi inlet dapat diimplementasikan sebagai fungsi Lambda, wadah, instans EC2 Amazon, atau sumber daya komputasi lainnya. Tidak perlu menjadi sumber daya cloud selama dapat memanggil ruang tunggu publik dan pribadiAPIs. Strategi inlet menerima peristiwa tentang ruang tunggu, situs web, atau indikator luar lainnya yang membantunya memutuskan kapan lebih banyak klien dapat mengeluarkan token dan memasuki situs. Ada beberapa pendekatan untuk strategi inlet. Yang mana yang Anda adopsi tergantung pada sumber daya yang tersedia untuk Anda dan kendala dalam desain situs web yang dilindungi.

Tindakan utama yang diambil oleh strategi inlet adalah memanggil `increment_serving_num` Amazon API Gateway pribadi API dengan nilai relatif yang menunjukkan berapa banyak lagi klien yang dapat memasuki situs. Bagian ini menjelaskan dua strategi inlet sampel. Ini dapat digunakan apa adanya, disesuaikan, atau Anda dapat menggunakan pendekatan yang sama sekali berbeda.

MaxSize

Dengan menggunakan MaxSize strategi ini, fungsi `MaxSizeInlet` Lambda dikonfigurasi dengan jumlah maksimum klien yang dapat menggunakan situs web secara bersamaan. Ini adalah nilai tetap. Klien mengeluarkan SNS notifikasi Amazon yang memanggil fungsi `MaxSizeInlet` Lambda untuk meningkatkan penghitung penayangan berdasarkan payload pesan. Sumber SNS pesan dapat datang dari mana saja, termasuk kode di situs web atau alat pemantauan yang mengamati tingkat pemanfaatan situs.

Fungsi `MaxSizeInlet` Lambda mengharapkan untuk menerima pesan yang dapat mencakup:

- `exited :`Jumlah transaksi yang telah selesai
- daftar permintaan IDs yang akan ditandai selesai
- daftar permintaan IDs yang akan ditandai ditinggalkan

Data ini digunakan untuk menentukan berapa banyak untuk menambah penghitung penyajian. Mungkin ada kasus di mana tidak ada kapasitas tambahan untuk menambah penghitung, berdasarkan jumlah klien saat ini.

Berkala

Saat menggunakan strategi periodik, CloudWatch aturan memanggil fungsi `PeriodicInlet` Lambda setiap menit untuk meningkatkan penghitung porsi dengan jumlah tetap. Saluran masuk periodik diparameterisasi dengan waktu mulai acara, waktu akhir, dan jumlah kenaikan. Secara opsional, strategi ini juga memeriksa CloudWatch alarm dan, jika alarm dalam `OK` keadaan, ia melakukan kenaikan, jika tidak maka akan melewatkannya. Integrator situs dapat menghubungkan metrik pemanfaatan ke alarm, dan menggunakan alarm itu untuk menjeda saluran masuk berkala. Strategi ini hanya mengubah posisi servis sementara waktu saat ini antara waktu mulai dan akhir, dan secara opsional, alarm yang ditentukan dalam `OK` keadaan.

Menyesuaikan dan memperluas solusi

Administrator situs organisasi Anda harus memutuskan metode integrasi yang akan digunakan dengan ruang tunggu. Ada dua opsi:

1. Integrasi dasar langsung menggunakan APIs dan otorisasi API Gateway.
2. Integrasi OpenID melalui penyedia identitas.

Selain integrasi di atas, Anda mungkin diminta untuk mengonfigurasi pengalihan nama domain. Anda juga bertanggung jawab untuk menyebarkan halaman situs ruang tunggu yang disesuaikan.

Ruang Tunggu Virtual pada AWS solusi dirancang untuk ekstensi melalui dua mekanisme: EventBridge untuk pemberitahuan acara searah dan REST APIs untuk komunikasi dua arah.

Kuota

Batasan skala utama untuk Ruang Tunggu Virtual aktif AWS adalah batas throttle Lambda untuk Wilayah yang diinstal. AWS Ketika diinstal ke AWS akun dengan kuota run bersamaan Lambda default, AWS solusi Ruang Tunggu Virtual dapat menangani hingga 500 klien per detik yang meminta posisi dalam antrian. Tarif 500 klien per detik didasarkan pada solusi yang memiliki semua batas kuota bersamaan fungsi Lambda tersedia secara eksklusif. Jika Wilayah di akun dibagikan dengan solusi lain yang menjalankan fungsi Lambda, Ruang Tunggu Virtual AWS pada solusi harus memiliki setidaknya 1.000 pemanggilan bersamaan yang tersedia. Anda dapat menggunakan CloudWatch metrik untuk memetakan pemanggilan Lambda secara bersamaan di akun Anda dari waktu ke waktu untuk membuat penentuan. Anda dapat menggunakan konsol Service Quotas untuk meminta peningkatan. Meningkatkan batas throttle Lambda hanya meningkatkan biaya akun bulanan jika pemanggilan tambahan benar-benar terjadi.

Untuk setiap tambahan 500 klien per detik, tingkatkan batas throttle Anda sebesar 1.000.

Pengguna masuk per detik diharapkan	Kuota eksekusi bersamaan yang direkomendasikan
0-500	1.000 (default)
501-1.000	2.000
1.001-1.500	3.000

Lambda memiliki batas burst tetap 3.000 pemanggilan bersamaan. Untuk informasi selengkapnya, lihat penskalaan fungsi Lambda. Kode klien harus mengharapkan dan mencoba lagi beberapa API panggilan jika kode kesalahan dikembalikan yang menunjukkan situasi throttle sementara. Contoh klien ruang tunggu menyertakan kode ini sebagai contoh bagaimana merancang klien yang digunakan dalam acara berkapasitas tinggi dan ledakan tinggi.

Solusi ini juga kompatibel dengan Lambda reserved dan provisioned concurrency dengan langkah-langkah konfigurasi kustom. Untuk detailnya, lihat Mengelola konkurensi cadangan Lambda.

Batas atas pengguna yang dapat memasuki ruang tunggu, menerima token, dan melanjutkan transaksi dibatasi oleh batas atas penghitung Elasticache (RedisOSS). Penghitung digunakan untuk posisi penyajian ruang tunggu dan melacak status ringkasan solusi. Penghitung yang digunakan dalam Elasticache (RedisOSS) memiliki batas atas 9.223.372.036,854.775.807. Tabel DynamoDB digunakan untuk menyimpan salinan setiap token yang dikeluarkan untuk pengguna ruang tunggu. DynamoDB tidak memiliki batasan praktis pada ukuran tabel.

Penyebaran regional

Layanan yang digunakan oleh solusi ini didukung di semua AWS Wilayah. Untuk ketersediaan AWS layanan terbaru berdasarkan Wilayah, lihat Daftar Layanan AWS Regional.

AWS CloudFormation template

Untuk mengotomatiskan penerapan, solusi ini menggunakan AWS CloudFormation templat berikut, yang dapat Anda unduh sebelum penerapan.

Jika ini adalah pertama kalinya menginstal, atau Anda tidak yakin apa yang harus diinstal, gunakan `virtual-waiting-room-on-aws-getting-started.template` AWS CloudFormation template, yang menginstal inti, otorisasi, dan contoh template kode ruang tunggu. Ini memungkinkan Anda untuk menguji ruang tunggu kerja dengan aliran sederhana.

View template

virtual-waiting-room-on- aws-api-gateway-cw -logs-role.template: Gunakan template ini untuk menambahkan peran default ke API Gateway di tingkat akun ARN untuk izin logging. CloudWatch Lihat Prasyarat untuk detail apakah akun Anda memerlukan penerapan templat ini atau tidak.

View template

virtual-waiting-room-on- aws-getting-started .template: Gunakan template bersarang ini untuk menginstal inti, otorisasi, dan contoh tumpukan ruang tunggu.

View template

virtual-waiting-room-on-aws.template: Gunakan template inti ini untuk menginstal layanan publik dan pribadi REST APIs dan cloud inti untuk membuat acara ruang tunggu. Instal template ini di akun dan Wilayah di mana Anda memerlukan ruang tunggu RESTAPIs, Elasticache (RedisOSS), dan tabel DynamoDB.

View template

virtual-waiting-room-on-aws-authorizers.template: Gunakan template ini untuk menginstal otorisasi Lambda yang dirancang untuk memverifikasi token yang dikeluarkan ruang tunggu dan dimaksudkan untuk melindungi pengguna akhir. APIs Membutuhkan tumpukan inti. Beberapa output dari tumpukan inti diperlukan sebagai parameter untuk menyebarkan tumpukan ini. Ini adalah template opsional.

View template

virtual-waiting-room-on-aws-openid.template: Gunakan template ini untuk menginstal penyedia identitas

OpenID untuk integrasi ruang tunggu dengan antarmuka otorisasi. Membutuhkan tumpukan inti. Beberapa output dari tumpukan inti diperlukan untuk menyebarkan tumpukan ini. Ini adalah template opsional.

View template

virtual-waiting-room-on- aws-sample-inlet-strategy .template: Gunakan template ini untuk menginstal strategi inlet sampel yang dimaksudkan untuk digunakan antara situs target dan ruang tunggu. Strategi masuk membantu merangkum logika untuk menentukan kapan mengizinkan lebih banyak pengguna masuk ke situs target. Membutuhkan tumpukan inti. Output dari tumpukan inti diperlukan untuk menyebarkan tumpukan ini. Ini adalah template opsional.

View template

virtual-waiting-room-on-aws-sample.template: Gunakan template ini untuk menginstal contoh web minimal dan konfigurasi API Gateway untuk ruang tunggu dan situs target. Membutuhkan tumpukan inti dan otorisasi. Output dari tumpukan inti dan otorisasi diperlukan sebagai parameter untuk menyebarkan tumpukan ini. Ini adalah template opsional.

Otomatisasi deployment

Sebelum Anda meluncurkan solusi, tinjau biaya, arsitektur, keamanan jaringan, dan pertimbangan lain yang dibahas dalam panduan ini. Ikuti step-by-step petunjuk di bagian ini untuk mengonfigurasi dan menyebarkan solusi ke akun Anda.

Waktu untuk menerapkan: Sekitar 30 menit (hanya memulai tumpukan)

Prasyarat

- AWS izin konsol akun yang setara dengan Akses Administrator.
- Aktifkan CloudWatch logging dari API Gateway:
  - Masuk ke konsol API Gateway dan pilih Wilayah tempat Anda berencana untuk menginstal tumpukan.

    Jika Anda sudah APIs didefinisikan di Wilayah ini:

    1. Pilih salah satuAPI.
    2. Dari navigasi kiri, pilih Pengaturan.
    3. Periksa nilai di ARN bidang peran CloudWatch log.

    - Jika tidak adaARN, instal`virtual-waiting-room-on-aws-api-gateway-cw-logs-role.template`.
    - Jika adaARN, mulailah dengan meluncurkan tumpukan yang memulai.

    Jika tidak ada yang APIs didefinisikan di Wilayah ini, instal file`virtual-waiting-room-on-aws-api-gateway-cw-logs-role.template`.
- Pengetahuan tentang arsitektur dan detail implementasi situs target untuk dilindungi.

Ikhtisar penyebaran

Gunakan langkah-langkah berikut untuk menerapkan solusi ini. AWS Untuk petunjuk terperinci, ikuti tautan untuk setiap langkah.

Langkah 1. Luncurkan tumpukan yang memulai

- Luncurkan AWS CloudFormation template ke AWS akun Anda.
- Tinjau parameter template dan masukkan atau sesuaikan nilai default sesuai kebutuhan.

Langkah 2. (Opsional) Uji ruang tunggu

- Hasilkan AWS kunci untuk memanggil yang IAM diamankanAPIs.
- Buka panel kontrol ruang tunggu sampel.
- Uji ruang tunggu sampel.

Langkah 1. Luncurkan tumpukan yang memulai

AWS CloudFormation Template otomatis ini menyebarkan template inti, otorisasi, dan contoh ruang tunggu yang memungkinkan Anda melihat dan menguji ruang tunggu yang berfungsi. Anda harus membaca dan memahami Prasyarat sebelum meluncurkan tumpukan.

> **Note**
>
> Anda bertanggung jawab atas biaya AWS layanan yang digunakan saat menjalankan solusi ini. Untuk detail selengkapnya, kunjungi bagian Biaya dalam panduan ini, dan lihat halaman web harga untuk setiap AWS layanan yang digunakan dalam solusi ini.

1. Masuk ke AWS Management Consoledan pilih tombol untuk meluncurkan `virtual-waiting-room-on-aws-getting-started.template` AWS CloudFormation template.

   Launch solution

   Atau, Anda dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri.
2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi di AWS Wilayah yang berbeda, gunakan pemilih Wilayah di bilah navigasi konsol.
3. Pada halaman Buat tumpukan, verifikasi bahwa template yang benar URL ada di kotak URL teks Amazon S3 dan pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat IAMdan STS Batas dalam Panduan AWS Identity and Access Management Pengguna.
5. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
ID Peristiwa	`Sample`	ID unik untuk contoh ruang tunggu ini, GUID format yang disarankan.
Masa Berlaku	`3600`	Periode validitas token dalam hitungan detik.
Aktifkan Generasi Acara	`false`	Jika disetel ke`true`, metrik yang terkait dengan Ruang Tunggu ditulis ke bus acara setiap menit
Pelabuhan Elasticache (OSSRedis)	`1785`	Nomor port yang digunakan untuk menghubungkan ke server Elasticache (RedisOSS). Disarankan untuk tidak menggunakan port Elasticache (RedisOSS) default dari. `6379`
EnableQueuePositionExpiry	`true`	Jika disetel ke`false`, periode kedaluwarsa posisi antrian tidak diterapkan.
QueuePositionExpiryPeriod	`900`	Ini adalah interval waktu dalam hitungan detik di mana posisi antrian tidak memenuhi syarat untuk menghasilkan token.

Parameter	Default	Deskripsi
IncrSvcOnQueuePosi tionExpiry	`false`	Jika disetel ke`true`, penghitung penayangan akan secara otomatis maju berdasarkan posisi antrian kedaluwarsa yang tidak berhasil menghasilkan token.

6. Pilih Berikutnya.
7. Pada Konfigurasikan halaman opsi stack, pilih Berikutnya.
8. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang mengakui bahwa template membuat AWS Identity and Access Management (IAM) sumber daya.
9. Pilih Membuat tumpukan untuk menerapkannya.

   Anda dapat melihat status tumpukan di AWS CloudFormation Konsol di kolom Status. Anda akan menerima COMPLETE status CREATE _ dalam waktu sekitar 30 menit.

Langkah 2. (Opsional) Uji ruang tunggu

Jika Anda menerapkan tumpukan memulai, langkah-langkah berikut membantu Anda menguji fungsionalitas ruang tunggu. Untuk menyelesaikan pengujian, Anda memerlukan AWS kunci dengan izin untuk memanggil yang IAM diamankan APIs di tumpukan inti.

Hasilkan AWS kunci untuk memanggil yang IAM diamankan APIs

1. Buat atau gunakan IAM pengguna di AWS akun tempat `aws-virtual-waiting-room-getting-started.template` CloudFormation templat digunakan.
2. Berikan akses terprogram IAM pengguna. Saat membuat satu set kunci akses baru untuk IAM pengguna, unduh file kunci saat disajikan. Anda memerlukan ID Kunci Akses dan Kunci Akses Rahasia IAM pengguna untuk menguji ruang tunggu.
3. Tambahkan IAM pengguna ke grup rotectedAPIGroup IAM pengguna P yang dibuat oleh template.

Buka panel kontrol ruang tunggu sampel

1. Masuk ke AWS CloudFormation konsol dan pilih tumpukan memulai solusi.

2. Pilih tab Output.
3. Di bawah kolom Kunci, cari ControlPanelURL, dan pilih nilai yang sesuai.
4. Buka panel kontrol di tab atau jendela browser baru.
5. Di panel kontrol, perluas bagian Konfigurasi.
6. Masukkan ID kunci Akses dan Kunci Akses Rahasia yang Anda ambil di Hasilkan AWS kunci untuk memanggil yang IAM diamankan APIs. Endpoint dan ID peristiwa diisi dari URL parameter.
7. Pilih Gunakan. Tombol diaktifkan setelah Anda memberikan kredensialnya.

Uji ruang tunggu sampel

1. Di AWS CloudFormation konsol, pilih tumpukan memulai solusi.
2. Pilih tab Output.
3. Di bawah kolom Kunci, cari WaitingRoomURL, dan pilih nilai yang sesuai.
4. Buka ruang tunggu, lalu pilih Reserve untuk masuk ke ruang tunggu.
5. Arahkan kembali ke tab browser yang memiliki panel kontrol.
6. Di bawah Penghitung Penyajian Kenaikan, pilih Ubah. Ini memungkinkan 100 pengguna untuk beralih dari ruang tunggu ke situs target.
7. Arahkan kembali ke ruang tunggu dan pilih Check out sekarang! Anda sekarang akan diarahkan ke situs target.
8. Pilih Beli sekarang untuk menyelesaikan transaksi Anda di situs target.

Menyebarkan tumpukan terpisah

Tumpukan inti adalah satu-satunya tumpukan yang diperlukan untuk mendapatkan fungsionalitas utama ruang tunggu. Semua tumpukan lainnya adalah opsional. Luncurkan tumpukan otorisasi jika Anda belum memiliki cara untuk memvalidasi token yang dikeluarkan ruang tunggu atau melindungi token yang mungkin sudah APIs Anda miliki. Luncurkan tumpukan OpenID jika Anda memerlukan penyedia identitas OpenID untuk integrasi ruang tunggu dengan antarmuka otorisasi. Contoh strategi inlet stack memberikan beberapa contoh tentang bagaimana dan kapan memungkinkan lebih banyak pengguna masuk ke situs yang Anda coba lindungi.

1. Luncurkan tumpukan inti

Waktu untuk menyebarkan: Sekitar 20 menit

AWS CloudFormation Template otomatis ini menyebarkan Ruang Tunggu Virtual AWS di AWS Cloud. Anda harus menyelesaikan Prasyarat sebelum meluncurkan tumpukan.

> **Note**
>
> Anda bertanggung jawab atas biaya AWS layanan yang digunakan saat menjalankan solusi ini. Untuk detail selengkapnya, kunjungi bagian Biaya dalam panduan ini, dan lihat halaman web harga untuk setiap AWS layanan yang digunakan dalam solusi ini.

1. Masuk ke AWS Management Consoledan pilih tombol untuk meluncurkan `aws-virtual-waiting-room-on-aws.template` AWS CloudFormation template.

   Launch solution Atau, Anda dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri.
2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi di AWS Wilayah yang berbeda, gunakan pemilih Wilayah di bilah navigasi konsol.
3. Pada halaman Buat tumpukan, verifikasi bahwa template yang benar URL ada di kotak URL teks Amazon S3 dan pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat IAMdan STS Batas dalam Panduan AWS Identity and Access Management Pengguna.

5. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
ID Peristiwa	`Sample`	ID unik untuk instance Ruang Tunggu ini, GUID format yang disarankan.
Masa Berlaku	`3600`	Periode validitas token dalam hitungan detik.
Aktifkan Generasi Acara	`false`	Jika disetel ke`true`, metrik yang terkait dengan ruang tunggu ditulis ke bus acara setiap menit.
Pelabuhan Elasticache (OSSRedis)	`1785`	Nomor port yang digunakan untuk menghubungkan ke server Elasticache (RedisOSS). Disarankan untuk tidak menggunakan port Elasticache (RedisOSS) default dari. `6379`
EnableQueuePositionExpiry	`true`	Jika disetel ke`false`, periode kedaluwarsa posisi antrian tidak diterapkan.
QueuePositionExpiryPeriod	`900`	Ini adalah interval waktu dalam hitungan detik di mana posisi antrian tidak memenuhi syarat untuk menghasilkan token.

Parameter	Default	Deskripsi
IncrSvcOnQueuePosi tionExpiry	`false`	Jika disetel `ketrue`, penghitung penayangan akan secara otomatis maju berdasarkan posisi antrian kedaluwarsa yang tidak berhasil menghasilkan token.

6. Pilih Berikutnya.
7. Pada Konfigurasikan halaman opsi stack, pilih Berikutnya.
8. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang mengakui bahwa template membuat AWS Identity and Access Management (IAM) sumber daya.
9. Pilih Membuat tumpukan untuk menerapkannya.

   Anda dapat melihat status tumpukan di AWS CloudFormation Konsol di kolom Status. Anda akan menerima COMPLETE status CREATE _ dalam waktu sekitar 20 menit.

2. (Opsional) Luncurkan tumpukan Authorizers

Waktu untuk menyebarkan: Sekitar lima menit

1. Masuk ke AWS Management Consoledan pilih tombol untuk meluncurkan `aws-virtual-waiting-room-on-aws-authorizers.template` AWS CloudFormation template.

   Atau, Anda dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri.
2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi di AWS Wilayah yang berbeda, gunakan pemilih Wilayah di bilah navigasi konsol.
3. Pada halaman Buat tumpukan, verifikasi bahwa template yang benar URL ada di kotak URL teks Amazon S3 dan pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat IAMdan STS Batas dalam Panduan AWS Identity and Access Management Pengguna.

5. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
Titik API Akhir Publik	*<Requires input>*	Titik akhir publik untuk ruang APIs tunggu virtual.
ID Acara Ruang Tunggu	`Sample`	ID acara ruang tunggu.
Penerbit URI	*<Requires input>*	Penerbit URI kunci publik dan token.

6. Pilih Berikutnya.
7. Pada Konfigurasikan halaman opsi stack, pilih Berikutnya.
8. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang mengakui bahwa template membuat AWS Identity and Access Management (IAM) sumber daya.
9. Pilih Membuat tumpukan untuk menerapkannya.

   Anda dapat melihat status tumpukan di AWS CloudFormation Konsol di kolom Status. Anda akan menerima COMPLETE status CREATE _ dalam waktu sekitar lima menit.

3. (Opsional) Luncurkan tumpukan OpenID

Waktu untuk menyebarkan: Sekitar lima menit

1. Masuk ke AWS Management Consoledan pilih tombol untuk meluncurkan `aws-virtual-waiting-room-on-aws-openid.template` AWS CloudFormation template.

   Launch solutionAtau,

   Anda dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri.
2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi di AWS Wilayah yang berbeda, gunakan pemilih Wilayah di bilah navigasi konsol.
3. Pada halaman Buat tumpukan, verifikasi bahwa template yang benar URL ada di kotak URL teks Amazon S3 dan pilih Berikutnya.

4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat IAMdan STS Batas dalam Panduan AWS Identity and Access Management Pengguna.
5. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
Titik API Akhir Publik	*<Requires input>*	Titik akhir publik URL untuk ruang APIs tunggu virtual.
Titik API Akhir Pribadi	*<Requires input>*	Titik akhir pribadi URL untuk ruang APIs tunggu virtual.
APIWilayah	*<Requires input>*	AWS nama wilayah untuk ruang tunggu publik dan pribadiAPIs.
ID Peristiwa	`Sample`	ID acara ruang tunggu.

6. Pilih Berikutnya.
7. Pada Konfigurasikan halaman opsi stack, pilih Berikutnya.
8. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang mengakui bahwa template membuat AWS Identity and Access Management (IAM) sumber daya.
9. Pilih Membuat tumpukan untuk menerapkannya.

   Anda dapat melihat status tumpukan di AWS CloudFormation Konsol di kolom Status. Anda akan menerima COMPLETE status CREATE _ dalam waktu sekitar lima menit.

4. (Opsional) Luncurkan tumpukan strategi inlet sampel

Waktu untuk menyebarkan: Sekitar dua menit

1. Masuk ke AWS Management Consoledan pilih tombol untuk meluncurkan `aws-virtual-waiting-room-sample-inlet-strategy.template` AWS CloudFormation template.

Launch solution Atau, Anda dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri.

2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi di AWS Wilayah yang berbeda, gunakan pemilih Wilayah di bilah navigasi konsol.
3. Pada halaman Buat tumpukan, verifikasi bahwa template yang benar URL ada di kotak URL teks Amazon S3 dan pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat IAMdan STS Batas dalam Panduan AWS Identity and Access Management Pengguna.
5. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
ID Peristiwa	`Sample`	ID acara ruang tunggu.
Titik API Akhir Inti Pribadi	*`<Requires input>`*	Titik akhir pribadi URL untuk ruang APIs tunggu virtual.
APIWilayah Inti	*`<Requires input>`*	AWS Wilayah tempat inti API dipasang.
Strategi Inlet	`Periodic`	Strategi inlet yang akan digunakan. `Periodic`menambah jumlah porsi setiap menit. `MaxSize`peningkatan jumlah penyajian berdasarkan jumlah maksimum transaksi yang dapat ditangani oleh situs target hilir pada waktu tertentu.
Kenaikan Oleh	*`<Requires input>`*	Berapa banyak konter penyajian harus ditambah

Parameter	Default	Deskripsi
		setiap menit. Diperlukan jika memilih strategi inlet periodik.
Waktu mulai	*<Requires input>*	Stempel waktu kapan harus mulai menambah nomor penyajian (waktu epoch dalam detik). Diperlukan jika memilih strategi inlet periodik.
Waktu Akhir	*<Requires input>*	Stempel waktu pada kapan harus berhenti menambah nomor penyajian (waktu epoch dalam detik). Jika dibiarkan 0, nomor penyajian bertambah tanpa batas waktu. Diperlukan jika memilih strategi inlet periodik.
CloudWatch Nama Alarm	*<Requires input>*	Nama CloudWatch alarm opsional untuk dikaitkan dengan strategi inlet periodik. Jika disediakan dan dalam keadaan mengkhawatirkan, jumlah penyajian tidak bertambah. Hanya berlaku untuk strategi inlet periodik.
Ukuran Maks	*<Requires input>*	Jumlah maksimum transaksi yang dapat diproses oleh situs target hilir sekaligus (MaxSize Strategi).

6. Pilih Berikutnya.
7. Pada Konfigurasikan halaman opsi stack, pilih Berikutnya.
8. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang mengakui bahwa template membuat AWS Identity and Access Management (IAM) sumber daya.

9. Pilih Membuat tumpukan untuk menerapkannya.

   Anda dapat melihat status tumpukan di AWS CloudFormation Konsol di kolom Status. Anda akan menerima COMPLETE status CREATE _ dalam waktu sekitar dua menit.

5. (Opsional) Luncurkan tumpukan ruang tunggu sampel

Waktu untuk menyebarkan: Sekitar lima menit

1. Masuk ke AWS Management Consoledan pilih tombol untuk meluncurkan `aws-virtual-waiting-room-sample.template` AWS CloudFormation template.

   Launch solution Atau,

   Anda dapat mengunduh template sebagai titik awal untuk implementasi Anda sendiri.
2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi di AWS Wilayah yang berbeda, gunakan pemilih Wilayah di bilah navigasi konsol.
3. Pada halaman Buat tumpukan, verifikasi bahwa template yang benar URL ada di kotak URL teks Amazon S3 dan pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat IAMdan STS Batas dalam Panduan AWS Identity and Access Management Pengguna.
5. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
APIWilayah Gateway	*<Requires input>*	AWS Nama wilayah API Gateway.
Pengotorisasi ARN	*<Requires input>*	ARNdari otorisasi API Gateway Lambda.
ID Peristiwa	`Sample`	ID acara ruang tunggu.

Parameter	Default	Deskripsi
Titik API Akhir Pribadi	*<Requires input>*	Titik akhir pribadi URL untuk ruang APIs tunggu virtual.
Titik API Akhir Publik	*<Requires input>*	Titik akhir publik URL untuk ruang APIs tunggu virtual.

6. Pilih Berikutnya.
7. Pada Konfigurasikan halaman opsi stack, pilih Berikutnya.
8. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Centang kotak yang mengakui bahwa template membuat AWS Identity and Access Management (IAM) sumber daya.
9. Pilih Membuat tumpukan untuk menerapkannya.

   Anda dapat melihat status tumpukan di AWS CloudFormation Konsol di kolom Status. Anda akan menerima COMPLETE status CREATE _ dalam waktu sekitar lima menit.

Memperbarui tumpukan dari versi sebelumnya

Kami merekomendasikan menghapus tumpukan dan membuat tumpukan baru untuk versi baru. Saat ini, migrasi ke versi yang lebih baru menggunakan pembaruan CloudFormation tumpukan tidak didukung. Lihat Copot pemasangan solusinya kemudian Luncurkan tumpukan memulai.

> **Note**
>
> Kami merekomendasikan migrasi ke versi yang lebih baru ketika Anda tidak aktif menggunakan solusi untuk mendukung acara yang sedang berlangsung.

Data kinerja

Virtual Waiting Room on AWS telah diuji beban dengan alat yang disebut Locust. Ukuran acara simulasi berkisar antara 10.000 hingga 100.000 klien. Lingkungan pengujian beban terdiri dari konfigurasi berikut:

- Locust 2.x dengan penyesuaian untuk penerapan Cloud AWS
- Empat AWS Wilayah (`us-west-1`,`us-west-2`,`us-east-1`,`us-east-2`)
- 10 host `c5.4xlarge` Amazon EC2 per Wilayah (total 40)
- 32 proses belalang per host
- Pengguna simulasi tersebar merata di antara 1.280 proses

Langkah-langkah pengujian end-to-end API untuk setiap proses pengguna:

1. Hubungi `assign_queue_num` dan terima ID permintaan.
2. Loop `queue_num` dengan ID permintaan hingga mengembalikan posisi antrian pengguna (waktu singkat).
3. Loop `serving_num` sampai nilai yang dikembalikan adalah >= posisi antrian pengguna (lama).
4. Jarang menelepon `waiting_room_size` untuk mengambil jumlah pengguna yang menunggu.
5. Panggil `generate_token` dan terima JWT untuk digunakan di situs target.

Temuan

Tidak ada batasan praktis untuk jumlah klien yang dapat diproses melalui ruang tunggu.

Tingkat di mana pengguna memasuki ruang tunggu memengaruhi kuota fungsi Lambda yang dijalankan secara bersamaan untuk Wilayah tempat Lambda digunakan.

Uji beban tidak dapat melebihi batas permintaan API Gateway default sebesar 10.000 permintaan per detik dengan kebijakan caching yang digunakan. CloudFront

Fungsi `get_queue_num` Lambda memiliki tingkat pemanggilan mendekati 1:1 dengan tingkat pengguna yang masuk ke ruang tunggu. Fungsi Lambda ini dapat dibatasi selama tingkat tinggi pengguna masuk karena batas konkurensi atau batas burst. Pelambatan yang disebabkan oleh sejumlah besar pemanggilan fungsi `get_queue_num` Lambda dapat memengaruhi fungsi Lambda

lainnya sebagai efek samping. Sistem keseluruhan terus beroperasi jika perangkat lunak klien dapat merespons dengan tepat jenis kesalahan penskalaan sementara ini dengan logika retry/back-off.

CloudFront Distribusi yang dikonfigurasi oleh tumpukan inti dalam konfigurasi kuota default dapat menangani ruang tunggu yang menampung 250.000 pengguna dengan setiap pengguna melakukan polling `serving_num` API setidaknya setiap detik.

Pemecahan Masalah

Bagian ini menyediakan informasi pemecahan masalah untuk solusi ini.

Jika bagian ini tidak membahas masalah Anda, Hubungi AWS Support memberikan petunjuk untuk membuka kasus AWS Support untuk solusi ini.

Status respons 4xx dari API

- Ini dapat disebabkan oleh ID Peristiwa atau ID Permintaan yang salah atau keduanya. Ini terjadi di CloudWatch Log untuk fungsi Lambda terkait.
- API pribadi diautentikasi oleh IAM dan klien membutuhkan AWS kunci yang memiliki hak untuk memanggil API pribadi. Ini terjadi di CloudWatch Log untuk API Gateway.

Status respons 5xx dari API

- Tanggapan dari Lambda atau API Gateway yang dibatasi, periksa alarm. *<LambdaFunctionName>*`ThrottlesAlarm` CloudWatch
- Kesalahan konfigurasi pada back-end, periksa *<LambdaFunctionName>*`ErrorsAlarm` CloudWatch alarm dan CloudWatch Log untuk detailnya.

5XX/ErrorPublicPrivateApiAlarm

- Status alarm ini adalah `ALARM` saat API mengembalikan status 5XX ke penelepon dalam periode 60 detik.
- Alarm ini kembali ke `OK` saat tidak ada status 5xx yang dikembalikan selama 60 detik.
- Alarm ini dapat dimulai dengan fungsi Lambda atau runtime Lambda yang mengembalikan kesalahan ke API Gateway.

4XX/ErrorPublicPrivateApiAlarm

- Status alarm ini adalah `ALARM` saat API mengembalikan status 4XX ke penelepon dalam periode 60 detik.
- Alarm ini kembali ke `OK` kapan status 4XX dikembalikan selama 60 detik.
- Alarm ini dapat diprakarsai oleh URL API yang salah.

*<LambdaFunctionName>*ThrottlesAlarm

- Status alarm ini adalah ALARM ketika Lambda bernama menemukan batas run bersamaan dalam periode 60 detik.
- Alarm ini kembali ke OK jika tidak ada throttle yang ditemui selama 60 detik.
- Anda mungkin perlu meningkatkan batas konkurensi untuk Wilayah akun Anda.
- Anda mungkin menghadapi batas burst untuk Lambda, yang memerlukan beberapa logika coba lagi pada klien Anda.

*<LambdaFunctionName>*ErrorsAlarm

- Status alarm ini adalah `ALARM` ketika Lambda bernama menemukan kesalahan runtime run dalam periode 60 detik.
- Alarm ini kembali ke OK jika tidak ada kesalahan yang ditemui selama 60 detik.
- Hal ini dapat disebabkan oleh kesalahan konfigurasi pada backend.
- Ini dapat disebabkan oleh bug dalam kode Lambda.

Kontak AWS Support

Jika Anda memiliki AWS Developer Support, AWS Business Support, atau AWS Enterprise Support, Anda dapat menggunakan Support Center untuk mendapatkan bantuan ahli terkait solusi ini. Bagian berikut memberikan petunjuk.

Buat kasus

1. Masuk ke Support Center.
2. Pilih Buat kasus.

Bagaimana kami bisa membantu?

1. Pilih Teknis.
2. Untuk Layanan, pilih Solusi.
3. Untuk Kategori, pilih Solusi Lain.
4. Untuk Keparahan, pilih opsi yang paling cocok dengan kasus penggunaan Anda.

5. Saat Anda memasukkan Layanan, Kategori, dan Tingkat Keparahan, antarmuka akan mengisi tautan ke pertanyaan pemecahan masalah umum. Jika Anda tidak dapat menyelesaikan pertanyaan Anda dengan tautan ini, pilih Langkah selanjutnya: Informasi tambahan.

Informasi tambahan

1. Untuk Subjek, masukkan teks yang merangkum pertanyaan atau masalah Anda.
2. Untuk Deskripsi, jelaskan masalah ini secara rinci.
3. Pilih Lampirkan file.
4. Lampirkan informasi yang AWS Support diperlukan untuk memproses permintaan.

Bantu kami menyelesaikan kasus Anda lebih cepat

1. Masukkan informasi yang diminta.
2. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.

Selesaikan sekarang atau hubungi kami

1. Tinjau solusi Selesaikan sekarang.
2. Jika Anda tidak dapat menyelesaikan masalah Anda dengan solusi ini, pilih Hubungi kami, masukkan informasi yang diminta, dan pilih Kirim.

Sumber daya tambahan

AWS layanan	
• AWS CloudFormation	• Amazon DynamoDB
• Layanan Penyimpanan Sederhana Amazon	• APIGerbang Amazon
• AWS Lambda	• AWS Secrets Manager
• Amazon CloudFront	• Layanan Antrian Sederhana Amazon
• Amazon EventBridge	• Amazon CloudWatch
• Elastisakit (Redis) OSS	• Amazon Comprehend
• Amazon Virtual Private Cloud	• AWS Identity and Access Management

Copot pemasangan solusinya

Anda dapat menghapus instalasi Ruang Tunggu Virtual pada AWS solusi dari AWS Management Console atau dengan menggunakan. AWS Command Line Interface Anda harus secara manual menghapus bucket S3 yang digunakan untuk menyimpan log oleh berbagai sumber daya yang dibuat oleh solusi ini. AWS Implementasi Solusi tidak secara otomatis menghapus bucket S3 ini sehingga Anda masih memiliki kemampuan untuk meninjau peristiwa log setelah solusi dihapus.

Jika Anda telah menambahkan pengguna IAM secara manual ke grup pengguna `ProtectedAPIGroup` IAM yang dibuat oleh solusi, hapus pengguna IAM dari grup pengguna IAM sebelum menghapus instalan solusi. Jika tidak, grup pengguna IAM dan kebijakan IAM terkait gagal dihapus.

Untuk setiap tumpukan yang digunakan, ikuti petunjuk di bawah ini.

Menggunakan AWS Management Console

1. Masuk ke konsol AWS CloudFormation tersebut.
2. Pada halaman Stacks, pilih tumpukan instalasi solusi ini.
3. Pilih Hapus.

Menggunakan AWS Command Line Interface

Tentukan apakah AWS Command Line Interface (AWS CLI) tersedia di lingkungan Anda. Untuk petunjuk pemasangan, lihat Apa itu AWS Command Line Interface? dalam AWS CLI User Guide. Setelah mengonfirmasi bahwa AWS CLI tersedia, jalankan perintah berikut.

```
$ aws cloudformation delete-stack --stack-name <installation-stack-name>
```

Menghapus bucket Amazon S3

Solusi ini dikonfigurasi untuk mempertahankan bucket Amazon S3 yang dibuat solusi (untuk diterapkan di Wilayah keikutsertaan) jika Anda memutuskan untuk menghapus tumpukan untuk mencegah kehilangan data yang tidak disengaja. AWS CloudFormation Setelah menghapus instalan solusi, Anda dapat menghapus bucket S3 ini secara manual jika Anda tidak perlu menyimpan data. Ikuti langkah-langkah ini untuk menghapus bucket Amazon S3.

1. Masuk ke konsol Amazon S3.
2. Pilih Bucket dari panel navigasi kiri.
3. Temukan ember <stack-name>S3.
4. Pilih bucket S3 dan pilih Delete.

Untuk menghapus bucket S3 menggunakan AWS CLI, jalankan perintah berikut:

```
$ aws s3 rb s3://<bucket-name> --force
```

Kode sumber

Kunjungi GitHubrepositori kami untuk mengunduh file sumber untuk solusi ini dan untuk berbagi penyesuaian Anda dengan orang lain.

Kontributor

- Jim Tharo
- Tiag Ramachandran
- Joan Morgan
- Justin Bajak Laut
- Allen Moheimani
- Garvit Singh
- Bassem Wani

Revisi

Tanggal	Perubahan
November 2021	Rilis awal
September 2022	Versi 1.1: Kenaikan penghitung penyajian otomatis berdasarkan posisi antrian kedaluwarsa. Pindahkan beberapa OSS penggunaan Elasticache (Redis) ke DynamoDB. APITitik akhir publik untuk mendapatkan waktu kedaluwarsa posisi antrian yang tersisa. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
April, 2023	Versi 1.1.1: Dampak yang dikurangi yang disebabkan oleh pengaturan default baru untuk Kepemilikan Objek S3 (ACLsdinonaktifkan) untuk semua bucket S3 baru. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
November 2023	Versi 1.1.2: Versi paket yang diperbarui untuk mengatasi kerentanan keamanan. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Maret 2024	Versi 1.1.3: Mengatasi tiga masalah: posisi antrian kedaluwarsa bertahan dalam ukuran ruang tunggu, `queue_num` API mengembal ikan hasil lama bahkan setelah reset, dan kegagalan intermiten di adaptor OpenID. `/userInfo` API Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
April 2024	Versi 1.1.4: Versi paket yang diperbarui untuk mengatasi kerentanan keamanan. Untuk

Tanggal	Perubahan
	informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Juni 2024	Versi 1.1.5: Versi paket yang diperbarui untuk mengatasi kerentanan keamanan. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Agustus 2024	Versi 1.1.6: Versi paket yang diperbarui untuk mengatasi kerentanan keamanan. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Agustus 2024	Versi 1.1.7: Versi paket yang diperbarui untuk mengatasi kerentanan keamanan. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
September 2024	Versi 1.1.8: Versi paket yang diperbarui untuk mengatasi kerentanan keamanan. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. AWS produk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau kondisi apa pun, baik tersurat maupun tersirat. AWS tanggung jawab dan kewajiban kepada pelanggannya dikendalikan oleh AWS perjanjian, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Ruang Tunggu Virtual AWS dilisensikan berdasarkan ketentuan Lisensi Apache Versi 2.0.

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