aws

Panduan Administrasi

Browser WorkSpaces Aman Amazon

Browser WorkSpaces Aman Amazon: Panduan Administrasi

Table of Contents

Apa itu Amazon WorkSpaces Secure Browser? 1
Riwayat rilis 1
Ketentuan yang perlu diketahui saat menggunakan Browser WorkSpaces Aman 2
Layanan terkait 4
Arsitektur 4
Mengakses Browser WorkSpaces Aman 5
Menyiapkan Browser WorkSpaces Aman 6
Mendaftar dan membuat pengguna 6
Mendaftar untuk Akun AWS 6
Buat pengguna dengan akses administratif 7
Memberikan akses terprogram 8
Jaringan dan akses 9
Persyaratan VPC 10
Rekomendasi pengaturan VPC 21
Zona Ketersediaan yang Didukung 23
Koneksi VPC 25
Koneksi klien/pengguna 25
Memulai dengan Browser WorkSpaces Aman 28
Langkah 1: Buat portal web 28
Konfigurasikan pengaturan jaringan 29
Konfigurasikan pengaturan portal 29
Konfigurasikan pengaturan pengguna 31
Konfigurasikan penyedia identitas 32
Tinjau dan luncurkan 43
Langkah 2: Uji portal web Anda 43
Langkah 3: Mendistribusikan portal web Anda 44
Langkah selanjutnya 44
Mengelola portal web Anda 45
Lihat detail portal web 45
Mengedit portal web 45
Hapus portal web 46
Kelola kuota layanan untuk portal Anda 46
Minta peningkatan portal 48
Minta peningkatan sesi bersamaan maksimum 48

Batasi contoh ... 49
Kelola kuota layanan ... 49
Kuota layanan lainnya ... 49
Kontrol interval untuk mengautentikasi ulang token IDP SAMP ... 50
Siapkan pencatatan akses pengguna ... 51
Log sampel ... 52
Menyetel atau mengedit kebijakan browser ... 53
Menetapkan kebijakan browser kustom (contoh) ... 54
Edit kebijakan browser dasar ... 60
Konfigurasikan Input Method Editor (IME) ... 62
Konfigurasikan lokalisasi dalam sesi ... 63
Mengatur kontrol akses IP (opsional) ... 66
Buat grup kontrol akses IP ... 66
Kaitkan pengaturan akses IP dengan portal web ... 67
Edit grup kontrol akses IP ... 68
Menghapus grup kontrol akses IP ... 68
Aktifkan ekstensi untuk sistem masuk tunggal (opsional) ... 69
Mengatur pemfilteran URL ... 71
Izinkan tautan dalam (opsional) ... 72
Keamanan ... 74
Perlindungan data ... 75
Enkripsi data ... 76
Privasi lalu lintas antar jaringan ... 78
Pencatatan akses pengguna ... 78
Identity and Access Management ... 78
Audiens ... 79
Mengautentikasi dengan identitas ... 80
Mengelola akses menggunakan kebijakan ... 83
Bagaimana Amazon WorkSpaces Secure Browser bekerja dengan IAM ... 86
Contoh kebijakan berbasis identitas ... 93
AWS kebijakan terkelola ... 96
Pemecahan Masalah ... 106
Menggunakan Peran Terkait Layanan ... 108
Respons insiden ... 112
Validasi kepatuhan ... 112
Ketangguhan ... 113

Keamanan infrastruktur 114
Konfigurasi dan analisis kerentanan 115
Praktik terbaik keamanan 115
Pemantauan 117
Pemantauan CloudWatch dengan 118
CloudTrail log 119
WorkSpaces Amankan informasi Browser di CloudTrail 120
Memahami entri file log Browser WorkSpaces Aman 121
Pencatatan akses pengguna 122
Panduan untuk pengguna Browser WorkSpaces Aman 124
Kompatibilitas browser dan perangkat 124
Akses portal web 125
Bimbingan sesi 125
Mulai sesi 125
Gunakan toolbar 126
Gunakan browser 129
Mengakhiri sesi 129
Pemecahan Masalah 130
Ekstensi untuk sistem masuk tunggal 131
Kompatibilitas 131
Penginstalan 132
Pemecahan Masalah 132
Riwayat dokumen 133
..... cxxxvii

Apa itu Amazon WorkSpaces Secure Browser?

> **Note**
>
> Amazon WorkSpaces Secure Browser sebelumnya dikenal sebagai Amazon WorkSpaces Web.

Amazon WorkSpaces Secure Browser adalah layanan browser yang dikelola sepenuhnya, cloud-native, dan dihosting yang digunakan untuk mengakses situs web pribadi dan aplikasi web (software-as-a-service SaaS) dengan aman, berinteraksi dengan sumber daya online, dan menjelajahi internet dari wadah sekali pakai. WorkSpaces Secure Browser bekerja dengan browser web pengguna yang ada, tanpa membebani TI dengan mengelola peralatan, infrastruktur, perangkat lunak klien khusus, atau koneksi jaringan pribadi virtual (VPN). Konten web dialirkan ke browser web pengguna, sedangkan browser dan konten web yang sebenarnya diisolasi. AWS Dengan menggunakan teknologi dasar yang sama yang mendukung layanan AWS End User Computing seperti Amazon WorkSpaces dan Amazon AppStream 2.0, WorkSpaces Secure Browser dapat lebih hemat biaya daripada desktop virtual tradisional, dan mengurangi kompleksitas dibandingkan dengan menyediakan perangkat lunak manajemen milik perusahaan. WorkSpaces Browser Aman mengurangi risiko eksfiltrasi data dengan streaming konten web. Tidak ada HTML, model objek dokumen (DOM), atau data perusahaan sensitif yang ditransmisikan ke mesin lokal. Dengan mengisolasi perangkat, jaringan perusahaan, dan internet dari satu sama lain, permukaan serangan browser hampir dihilangkan.

Anda dapat menerapkan kebijakan browser perusahaan (termasuk pengizinan/pemblokiran URL) pada semua sesi, dan menyertakan kontrol tingkat sesi untuk clipboard, transfer file, dan printer. Anda juga dapat membatasi akses ke jaringan atau perangkat tepercaya dengan menggunakan Kontrol Akses IP. WorkSpaces Browser Aman mudah diatur dan dioperasikan. Setiap sesi diluncurkan dengan versi Browser Chrome yang baru dan sepenuhnya ditambal, dengan kebijakan dan pengaturan perusahaan diterapkan.

Riwayat rilis

Pada 20 Mei 2024, Amazon WorkSpaces Web diubah namanya menjadi Amazon WorkSpaces Secure Browser. Untuk pelanggan yang sudah ada, tidak ada perubahan pada cara mereka mengelola pengguna atau sumber daya dengan layanan. Daftar berikut menjelaskan pembaruan yang berlaku yang juga terjadi sebagai akibat dari penggantian nama ini.

Namespace API web ruang kerja tetap tidak berubah untuk kompatibilitas mundur. Akibatnya, sumber daya berikut masih sama:

- Perintah CLI.
- CloudWatch Metrik Amazon. Untuk informasi selengkapnya, lihat the section called “Pemantauan CloudWatch dengan”.
- Titik akhir layanan. Untuk informasi selengkapnya, lihat titik akhir dan kuota Amazon WorkSpaces Secure Browser.
- AWS CloudFormation sumber daya. Untuk informasi selengkapnya, lihat referensi jenis sumber daya Amazon WorkSpaces Secure Browser.
- Peran terkait layanan yang berisi ruang kerja-web. Untuk informasi selengkapnya, lihat the section called “Menggunakan Peran Terkait Layanan”.
- URL konsol yang berisi workspaces-web.
- URL dokumentasi yang berisi workspaces-web. Untuk informasi selengkapnya, lihat Dokumentasi Browser WorkSpaces Aman Amazon.
- Peran ReadOnly terkelola yang ada. Untuk informasi selengkapnya, lihat the section called “AWS kebijakan terkelola”.
- Nama hibah KMS.
- UAL (Pencatatan Aktivitas Pengguna) Awalan aliran Kinesis.

Selain itu, URL portal yang ada tetap sama. <UUID>URL untuk portal yang dibuat sebelum 20 Mei 2024 menggunakan format.workspaces-web.com. WorkSpaces Portal Browser Aman terus menggunakan format ini dan domain workspaces-web.com.

Ketentuan yang perlu diketahui saat menggunakan Browser WorkSpaces Aman

Untuk membantu Anda memulai dengan Browser WorkSpaces Aman, Anda harus terbiasa dengan konsep-konsep berikut.

Penyedia identitas (iDP)

> Penyedia identitas memverifikasi kredensyal pengguna Anda. Kemudian mengeluarkan pernyataan otentikasi untuk menyediakan akses ke penyedia layanan. Anda dapat mengonfigurasi IDP yang ada untuk bekerja dengan Browser WorkSpaces Aman.

Proses untuk mengonfigurasi penyedia identitas Anda (iDP) bervariasi, tergantung pada IDP Anda.

Anda harus mengunggah file metadata penyedia layanan ke IDP Anda. Jika tidak, pengguna Anda tidak akan dapat masuk. Anda juga harus memberikan akses kepada pengguna Anda untuk menggunakan Browser WorkSpaces Aman di IDP Anda.

Dokumen metadata penyedia identitas (iDP)

WorkSpaces Browser Aman memerlukan metadata khusus dari penyedia identitas Anda (IDP) untuk membangun kepercayaan. Anda dapat menambahkan metadata ini ke Browser WorkSpaces Aman dengan mengunggah file pertukaran metadata yang diunduh dari IDP Anda.

Penyedia layanan (SP)

Penyedia layanan menerima pernyataan otentikasi dan menyediakan layanan kepada pengguna. WorkSpaces Secure Browser bertindak sebagai penyedia layanan untuk pengguna yang telah diautentikasi oleh IDP mereka.

Dokumen metadata penyedia layanan (SP)

Anda perlu menambahkan detail metadata penyedia layanan ke antarmuka konfigurasi penyedia identitas (IDP) Anda. Rincian proses konfigurasi ini bervariasi antar penyedia.

SAML 2.0

Standar untuk bertukar data otentikasi dan otorisasi antara IDP dan penyedia layanan.

Cloud Privat Virtual (VPC)

Anda dapat menggunakan VPC yang sudah ada atau baru, subnet yang sesuai, dan grup keamanan untuk menautkan konten Anda dengan WorkSpaces Browser Aman.

Subnet harus dengan koneksi yang stabil ke internet, dan VPC dan subnet juga harus memiliki koneksi yang stabil ke situs web internal dan Perangkat Lunak sebagai Layanan (SaaS) bagi pengguna untuk mengakses sumber daya ini.

VPC, subnet, dan grup keamanan yang terdaftar diambil dari wilayah yang sama dengan konsol Browser WorkSpaces Aman Anda.

Toko kepercayaan

Jika pengguna yang mengakses situs web melalui Browser WorkSpaces Aman menerima kesalahan privasi, seperti NET: :ERR_CERT_INVALID, situs tersebut mungkin menggunakan

sertifikat yang ditandatangani oleh otoritas sertifikat pribadi (PCA). Anda mungkin perlu menambahkan atau mengubah PCA di toko kepercayaan Anda. Selain itu, jika perangkat pengguna mengharuskan Anda untuk menginstal sertifikat tertentu untuk memuat situs web, Anda perlu menambahkan sertifikat itu ke toko kepercayaan Anda untuk memungkinkan pengguna mengakses situs tersebut di Browser WorkSpaces Aman.

Situs web yang dapat diakses publik biasanya tidak memerlukan perubahan apa pun ke toko kepercayaan.

Portal web

Portal web memberi pengguna Anda akses ke situs web internal dan SaaS dari browser mereka. Anda dapat membuat satu portal web di setiap wilayah yang didukung per akun. Untuk meminta peningkatan batas untuk lebih dari satu portal, hubungi dukungan.

Titik akhir portal web

Titik akhir portal web adalah titik akses pengguna Anda akan meluncurkan portal web Anda setelah masuk dengan penyedia identitas yang dikonfigurasi untuk portal.

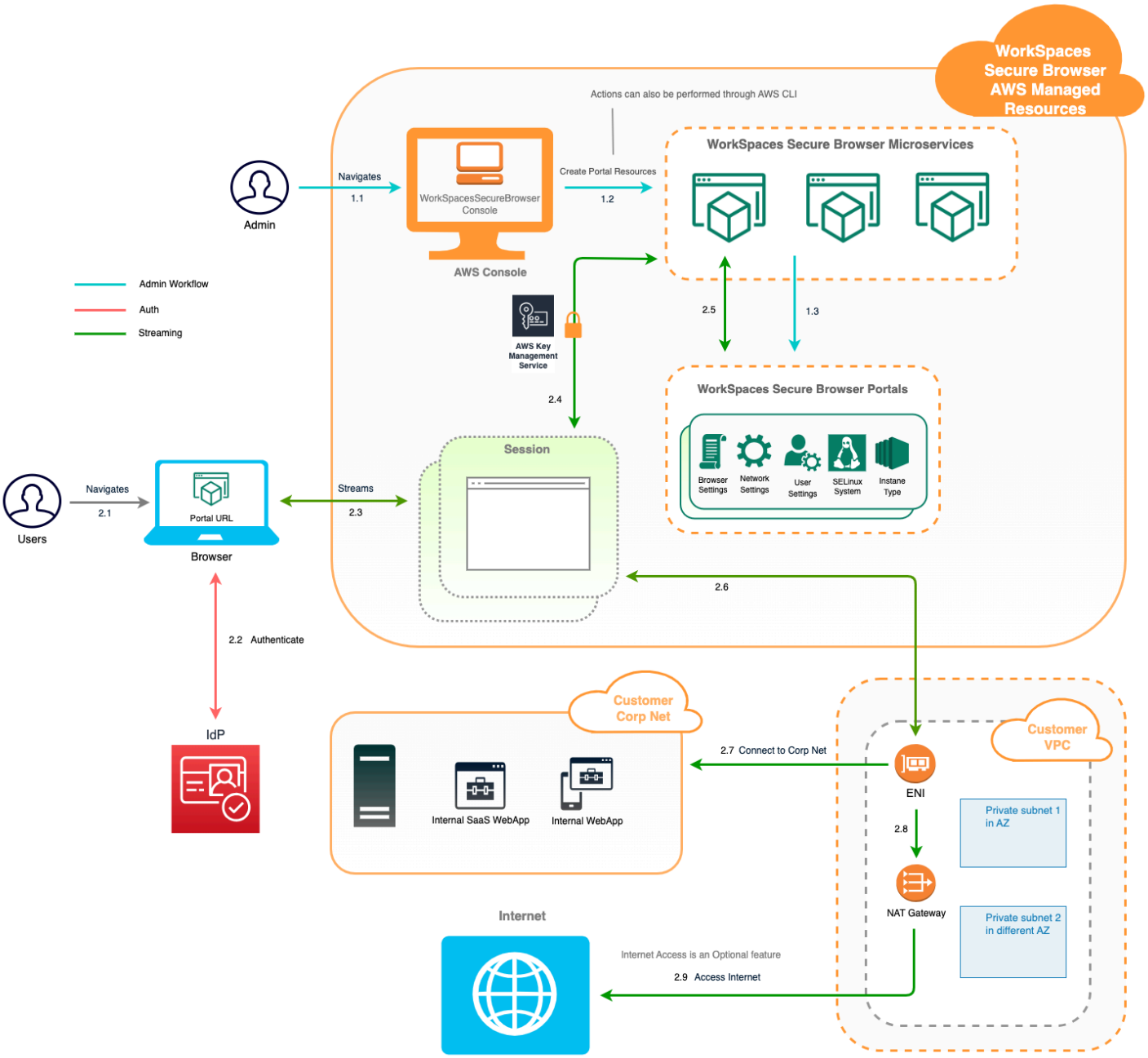
Titik akhir tersedia untuk umum di internet dan dapat disematkan ke jaringan Anda.

Layanan terkait

WorkSpaces Secure Browser adalah kemampuan dari Amazon WorkSpaces dalam portofolio AWS End User Computing. Dibandingkan dengan WorkSpaces dan AppStream 2.0, WorkSpaces Secure Browser dibangun khusus untuk memfasilitasi beban kerja berbasis web yang aman. WorkSpaces Browser Aman dikelola secara otomatis, dengan kapasitas, penskalaan, dan gambar disediakan dan diperbarui sesuai permintaan oleh AWS. Misalnya, Anda dapat memilih untuk menawarkan Desktop Ruang Kerja persisten kepada pengembang perangkat lunak Anda yang memerlukan akses ke sumber daya desktop, dan Browser WorkSpaces Aman ke pengguna pusat kontak yang hanya memerlukan akses ke beberapa situs web internal dan SaaS (termasuk yang dihosting di luar jaringan Anda) di komputer desktop.

Arsitektur

Diagram berikut menunjukkan arsitektur WorkSpaces Secure Browser.



Mengakses Browser WorkSpaces Aman

Administrator mengakses Browser WorkSpaces Aman melalui WorkSpaces Secure Browser Console, SDK, CLI, atau API. Pengguna Anda mengaksesnya melalui titik akhir Browser WorkSpaces Aman.

Menyiapkan Browser WorkSpaces Aman

Sebelum Anda dapat mengonfigurasi Browser WorkSpaces Aman untuk menjangkau situs web internal dan aplikasi SaaS Anda, Anda harus menyelesaikan prasyarat berikut.

Topik

- Mendaftar dan membuat pengguna
- Memberikan akses terprogram
- Jaringan dan akses

Mendaftar dan membuat pengguna

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimkan email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Pengguna root akun AWS

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

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Memberikan akses terprogram

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensyal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat autentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	Gunakan kredensyal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensi sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensyal jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensyal pengguna IAM di Panduan Pengguna.AWS Command Line Interface • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensi jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Jaringan dan akses

Topik berikut menjelaskan cara mengatur instance streaming Browser WorkSpaces Aman sehingga pengguna dapat terhubung dengannya. Ini juga menjelaskan cara mengaktifkan instance streaming Browser WorkSpaces Aman Anda untuk mengakses sumber daya VPC, serta internet.

Topik

- Persyaratan VPC
- Rekomendasi pengaturan VPC
- Zona Ketersediaan yang Didukung
- Koneksi VPC
- Koneksi klien/pengguna

Persyaratan VPC

Selama pembuatan portal Browser WorkSpaces Aman, Anda akan memilih VPC di akun Anda. Anda juga akan memilih setidaknya dua subnet di dua Availability Zone yang berbeda. VPC dan subnet ini harus memenuhi persyaratan berikut:

- VPC harus memiliki tenancy default. VPC dengan penyewaan khusus tidak didukung.
- Untuk pertimbangan ketersediaan, kami memerlukan setidaknya dua subnet yang dibuat di dua Availability Zone yang berbeda. Subnet Anda harus memiliki alamat IP yang cukup untuk mendukung lalu lintas Browser WorkSpaces Aman yang diharapkan. Konfigurasikan setiap subnet Anda dengan subnet mask yang memungkinkan alamat IP klien yang cukup untuk memperhitungkan jumlah maksimum sesi bersamaan. Untuk informasi selengkapnya, lihat Buat dan konfigurasikan VPC baru.
- Semua subnet harus memiliki koneksi yang stabil ke konten internal apa pun, baik yang terletak di AWS Cloud atau di tempat, yang akan diakses pengguna dengan Browser WorkSpaces Aman.

Kami menyarankan Anda memilih tiga subnet di Availability Zone yang berbeda untuk pertimbangan ketersediaan dan penskalaan. Untuk informasi selengkapnya, lihat Buat dan konfigurasikan VPC baru.

WorkSpaces Browser Aman tidak menetapkan alamat IP publik apa pun ke instans streaming untuk mengaktifkan akses internet. Ini akan membuat instance streaming Anda dapat diakses dari internet. Oleh karena itu, instans streaming apa pun yang terhubung ke subnet publik Anda tidak akan memiliki akses internet. Jika Anda ingin portal Browser WorkSpaces Aman Anda memiliki akses ke konten internet publik dan konten VPC pribadi, selesaikan langkah-langkahnya. Aktifkan penjelajahan internet tanpa batas (disarankan)

Buat dan konfigurasikan VPC baru

Bagian ini menjelaskan cara menggunakan wizard VPC untuk membuat VPC dengan satu subnet publik dan satu subnet pribadi. Sebagai bagian dari proses ini, wizard membuat gateway internet dan gateway NAT. Ini juga membuat tabel rute khusus yang terkait dengan subnet publik. Kemudian memperbarui tabel rute utama yang terkait dengan subnet pribadi. Gateway NAT secara otomatis dibuat di subnet publik VPC Anda.

Setelah Anda menggunakan wizard untuk membuat konfigurasi VPC, Anda akan menambahkan subnet pribadi kedua. Untuk informasi selengkapnya tentang konfigurasi ini, lihat VPC dengan subnet publik dan pribadi (NAT).

Langkah 1: Alokasikan sebuah alamat IP Elastis

Sebelum membuat VPC, Anda harus mengalokasikan alamat IP Elastis di Wilayah Browser WorkSpaces Aman Anda. Setelah dialokasikan, Anda dapat mengaitkan alamat IP Elastis dengan gateway NAT Anda. Dengan alamat IP Elastic, Anda dapat menutupi kegagalan instans streaming Anda dengan memetakan ulang alamat secara cepat ke instans streaming lain di VPC Anda. Untuk informasi selengkapnya, lihat Alamat IP elastis.

> **Note**
>
> Biaya mungkin berlaku untuk alamat IP Elastic yang Anda gunakan. Untuk informasi selengkapnya, lihat halaman harga alamat IP Elastis.

Jika Anda belum memiliki alamat IP Elastis, selesaikan langkah-langkah berikut. Jika Anda ingin menggunakan alamat IP Elastic yang ada, Anda harus terlebih dahulu memverifikasi bahwa itu saat ini tidak terkait dengan instance atau antarmuka jaringan lain.

Untuk mengalokasikan Alamat IP elastis

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, di bawah Jaringan & Keamanan, pilih IP Elastis.
3. Pilih Alokasikan Alamat Baru, lalu pilih Alokasikan.
4. Perhatikan alamat IP Elastis yang ditampilkan di konsol.
5. Di sudut kanan atas panel IP Elastis, klik ikon × untuk menutup panel.

Langkah 2: Buat VPC baru

Selesaikan langkah-langkah berikut untuk membuat VPC baru dengan satu subnet publik dan satu subnet pribadi.

Untuk membuat VPC baru

1. Buka Konsol VPC Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC Dasbor.
3. Pilih Peluncuran Wizard VPC.
4. Pada Langkah 1: Pilih Konfigurasi VPC, pilih VPC dengan Subnet Publik dan Pribadi, lalu pilih Pilih.
5. Pada Langkah 2: VPC dengan Subnet Publik dan Pribadi, konfigurasikan VPC sebagai berikut:
   - Untuk blok IPv4 CIDR, tentukan blok CIDR IPv4 untuk VPC.
   - Untuk blok IPv6 CIDR, pertahankan nilai default, Tidak ada Blok CIDR IPv6.
   - Untuk nama VPC, masukkan nama unik untuk VPC.
   - Konfigurasi subnet publik sebagai berikut:
     - Untuk IPv4 CIDR subnet Public, tentukan blok CIDR untuk subnet.
     - Untuk Availability Zone, pertahankan nilai default, No Preference.
     - Untuk nama subnet publik, masukkan nama untuk subnet. Misalnya, **`WorkSpaces Secure Browser Public Subnet`**.
   - Konfigurasi subnet privat sebagai berikut:
     - Untuk IPv4 CIDR subnet Private, tentukan blok CIDR untuk subnet. Catat nilai yang Anda tentukan.
     - Untuk Availability Zone, pilih zona tertentu dan catat zona yang Anda pilih.
     - Untuk nama subnet pribadi, masukkan nama untuk subnet. Misalnya, **`WorkSpaces Secure Browser Private Subnet1`**.
   - Untuk bidang yang tersisa, pertahankan nilai default jika berlaku.
   - Untuk ID Alokasi IP Elastis, masukkan nilai yang sesuai dengan alamat IP Elastis yang Anda buat. Alamat ini kemudian ditetapkan ke gateway NAT. Jika Anda tidak memiliki alamat IP Elastis, buat alamat IP dengan menggunakan Konsol VPC Amazon di https://console.aws.amazon.com/vpc/.
   - Untuk titik akhir Layanan, jika titik akhir Amazon S3 diperlukan untuk lingkungan Anda, tentukan satu.

Untuk menentukan titik akhir Amazon S3, lakukan hal berikut:

1. Pilih Tambahkan Titik Akhir.
2. Untuk Layanan, pilih com.amazonaws. Entri ***Region*** .s3, di mana *Region* adalah tempat Wilayah AWS Anda membuat VPC Anda.
3. Untuk Subnet, pilih Private subnet.
4. Untuk Kebijakan, pertahankan nilai default, Akses Penuh.

- Untuk Aktifkan nama host DNS, pertahankan nilai default, Ya.
- Untuk penyewaan Hardware, pertahankan nilai default, Default.
- Pilih Buat VPC.
- Dibutuhkan beberapa menit untuk mengatur VPC Anda. Setelah VPC dibuat, pilih OKE.

Langkah 3: Tambahkan subnet privat kedua

Pada langkah sebelumnya, Anda membuat VPC dengan satu subnet publik dan satu subnet privat. Selesaikan langkah-langkah berikut untuk menambahkan subnet pribadi kedua ke VPC Anda. Kami menyarankan Anda menambahkan subnet pribadi kedua di Availability Zone yang berbeda dari subnet pribadi pertama Anda.

Untuk menambahkan subnet pribadi kedua

1. Di panel navigasi, pilih Pengguna.
2. Pilih subnet pribadi pertama yang Anda buat di langkah sebelumnya. Pada tab Deskripsi, di bawah daftar subnet, buat catatan Availability Zone untuk subnet ini.
3. Di kiri atas panel subnet, pilih Create Subnet.
4. Untuk tag Nama, masukkan nama untuk subnet pribadi. Misalnya, **`WorkSpaces Secure Browser Private Subnet2`**.
5. Untuk VPC, pilih VPC yang Anda buat di langkah sebelumnya.
6. Untuk Availability Zone, pilih Availability Zone selain yang Anda gunakan untuk subnet pribadi pertama Anda. Memilih Availability Zone yang berbeda meningkatkan toleransi kesalahan dan membantu mencegah kesalahan kapasitas yang tidak mencukupi.
7. Untuk blok IPv4 CIDR, tentukan rentang blok CIDR unik untuk subnet baru. Misalnya, jika subnet pribadi pertama Anda memiliki rentang blok IPv4 CIDR**`10.0.1.0/24`**, Anda dapat menentukan rentang blok CIDR **`10.0.2.0/24`** untuk subnet pribadi kedua.
8. Pilih Buat.

9. Setelah subnet Anda dibuat, pilih Tutup.

Langkah 4: Verifikasi dan beri nama tabel rute subnet Anda

Setelah membuat dan mengonfigurasi VPC, selesaikan langkah-langkah berikut untuk menentukan nama tabel rute Anda. Anda harus memverifikasi bahwa detail berikut ini benar untuk tabel rute Anda:

- Tabel rute yang terkait dengan subnet tempat gateway NAT Anda berada harus menyertakan rute yang mengarahkan lalu lintas internet ke gateway internet. Ini memastikan bahwa gateway NAT Anda dapat mengakses internet.
- Tabel rute yang terkait dengan subnet pribadi Anda harus dikonfigurasi untuk mengarahkan lalu lintas internet ke gateway NAT. Ini memungkinkan contoh streaming di subnet pribadi Anda untuk berkomunikasi dengan internet.

Untuk memverifikasi dan memberi nama tabel rute subnet Anda

1. Di panel navigasi, pilih Subnet, lalu pilih subnet publik yang Anda buat. Misalnya, WorkSpaces Secure Browser 2.0 Public Subnet.
2. Pada tab Tabel rute, pilih ID tabel rute. Misalnya, rtb-12345678.
3. Pilih tabel rute. Di bawah Nama, pilih ikon edit (pensil), dan masukkan nama untuk tabel. Misalnya, masukkan nama**`workspacesweb-public-routetable`**. Kemudian pilih tanda centang untuk menyimpan nama.
4. Dengan tabel rute publik masih dipilih, pada tab Rute, verifikasi bahwa ada dua rute: satu untuk lalu lintas lokal, dan satu yang mengirim semua lalu lintas lainnya melalui gateway internet VPC. Tabel berikut menjelaskan dua rute ini:

Tujuan	Target	Deskripsi
Blok CIDR IPv4 subnet publik (misalnya, 10.0.0/20)	Lokal:	Semua lalu lintas dari sumber daya yang ditujukan untuk alamat IPv4 dalam blok CIDR IPv4 subnet publik. Lalu lintas ini diarahkan secara lokal di dalam VPC.

Tujuan	Target	Deskripsi
Lalu lintas ditujukan untuk semua alamat IPv4 lainnya (misalnya, 0.0.0.0/0)	Keluar (IGW-ID)	Lalu lintas yang ditujukan untuk semua alamat IPv4 lainnya dirutekan ke gateway internet (diidentifikasi oleh IGW-ID) yang dibuat oleh wizard VPC.

5. Di panel navigasi, pilih Pengguna. Kemudian, pilih subnet pribadi pertama yang Anda buat (misalnya,**`WorkSpaces Secure Browser Private Subnet1`**).
6. Pada tab Route Table, pilih ID tabel rute.
7. Pilih tabel rute. Di bawah Nama, pilih ikon edit (pensil), dan masukkan nama untuk tabel. Misalnya, masukkan nama**`workspacesweb-private-routetable`**. Kemudian pilih tanda centang untuk menyimpan nama.
8. Pada tab Rute, verifikasi bahwa tabel rute menyertakan rute berikut:

Tujuan	Target	Deskripsi
Blok CIDR IPv4 subnet publik (misalnya, 10.0.0/20)	Lokal:	Semua lalu lintas dari sumber daya yang ditujukan untuk alamat IPv4 dalam blok CIDR IPv4 subnet publik dirutekan secara lokal di dalam VPC.
Lalu lintas ditujukan untuk semua alamat IPv4 lainnya (misalnya, 0.0.0.0/0)	Keluar (Nat-ID)	Lalu lintas yang ditujukan untuk semua alamat IPv4 lainnya diarahkan ke gateway NAT (diidentifikasi oleh NAT-ID).
Lalu lintas yang ditujukan untuk bucket S3 (berlaku jika Anda menentukan titik	Penyimpanan (VPCE-ID)	Lalu lintas yang ditujukan untuk bucket S3 diarahkan ke titik akhir S3 (diidentifikasi oleh VPCE-ID).

Tujuan	Target	Deskripsi
akhir S3) [PL-ID (com.amazonaws.region.s3)]		

9. Di panel navigasi, pilih Pengguna. Kemudian pilih subnet pribadi kedua yang Anda buat (misalnya,**`WorkSpaces Secure Browser Private Subnet2`**).
10. Pada tab Route Table, verifikasi bahwa tabel rute yang dipilih adalah tabel rute pribadi (misalnya,**`workspacesweb-private-routetable`**). Jika tabel rute berbeda, pilih Edit dan pilih tabel rute pribadi Anda.

Aktifkan penjelajahan internet tanpa batas (disarankan)

Ikuti langkah-langkah ini untuk mengonfigurasi VPC dengan gateway NAT untuk penjelajahan internet tanpa batas. Ini memberikan akses Browser WorkSpaces Aman ke situs di internet publik, dan situs pribadi yang dihosting di atau dengan koneksi ke VPC Anda.

Untuk mengonfigurasi VPC dengan gateway NAT untuk penjelajahan internet tanpa batas

Jika Anda ingin portal Browser WorkSpaces Aman Anda memiliki akses ke konten internet publik dan konten VPC pribadi, ikuti langkah-langkah berikut:

> **Note**
>
> Jika Anda sudah mengonfigurasi VPC, selesaikan langkah-langkah berikut untuk menambahkan gateway NAT ke VPC Anda. Jika Anda perlu membuat VPC baru, lihat. Buat dan konfigurasikan VPC baru

1. Untuk membuat gateway NAT Anda, selesaikan langkah-langkah di Buat gateway NAT. Pastikan gateway NAT ini memiliki konektivitas publik, dan berada di subnet publik di VPC Anda.
2. Anda harus menentukan setidaknya dua subnet pribadi dari Availability Zone yang berbeda. Menetapkan subnet Anda ke Availability Zone yang berbeda membantu memastikan ketersediaan dan toleransi kesalahan yang lebih baik. Untuk informasi tentang cara membuat subnet pribadi kedua, lihatthe section called “Langkah 3: Tambahkan subnet privat kedua”.

> **Note**
>
> Untuk memastikan setiap instans streaming memiliki akses internet, jangan lampirkan subnet publik ke portal Browser WorkSpaces Aman Anda.

3. Perbarui tabel rute yang terkait dengan subnet pribadi Anda untuk mengarahkan lalu lintas ke internet ke gateway NAT. Ini memungkinkan contoh streaming di subnet pribadi Anda untuk berkomunikasi dengan internet. Untuk informasi tentang cara mengaitkan tabel rute dengan subnet pribadi, selesaikan langkah-langkah di Konfigurasi tabel rute.

Aktifkan penjelajahan internet terbatas (menggunakan proxy HTTP keluar)

Pengaturan jaringan yang direkomendasikan dari portal Browser WorkSpaces Aman adalah menggunakan subnet pribadi dengan gateway NAT, sehingga portal dapat menelusuri internet publik dan konten pribadi. Untuk informasi selengkapnya, lihat the section called “Aktifkan penjelajahan internet tanpa batas (disarankan)”. Namun, Anda mungkin diminta untuk mengontrol komunikasi keluar dari portal Browser WorkSpaces Aman ke internet dengan menggunakan proxy web. Misalnya, jika Anda menggunakan proxy web sebagai gateway ke internet, Anda dapat menerapkan kontrol keamanan preventif, seperti daftar izin domain dan pemfilteran konten. Ini juga dapat mengurangi penggunaan bandwidth dan meningkatkan kinerja jaringan dengan menyimpan sumber daya yang sering diakses, seperti halaman web atau pembaruan perangkat lunak secara lokal. Untuk beberapa kasus penggunaan, Anda mungkin memiliki konten pribadi yang hanya dapat diakses dengan menggunakan proxy web.

Anda mungkin sudah terbiasa dengan mengonfigurasi pengaturan proxy pada perangkat terkelola, atau pada gambar lingkungan virtual Anda. Tetapi ini menimbulkan tantangan jika Anda tidak mengendalikan perangkat (misalnya, ketika pengguna menggunakan perangkat yang tidak dimiliki atau dikelola oleh perusahaan), atau jika Anda perlu mengelola gambar untuk lingkungan virtual Anda. Dengan Browser WorkSpaces Aman, Anda dapat mengatur pengaturan proxy menggunakan kebijakan Chrome yang ada di browser web. Anda dapat melakukan ini dengan menyiapkan proxy keluar HTTP untuk Browser WorkSpaces Aman.

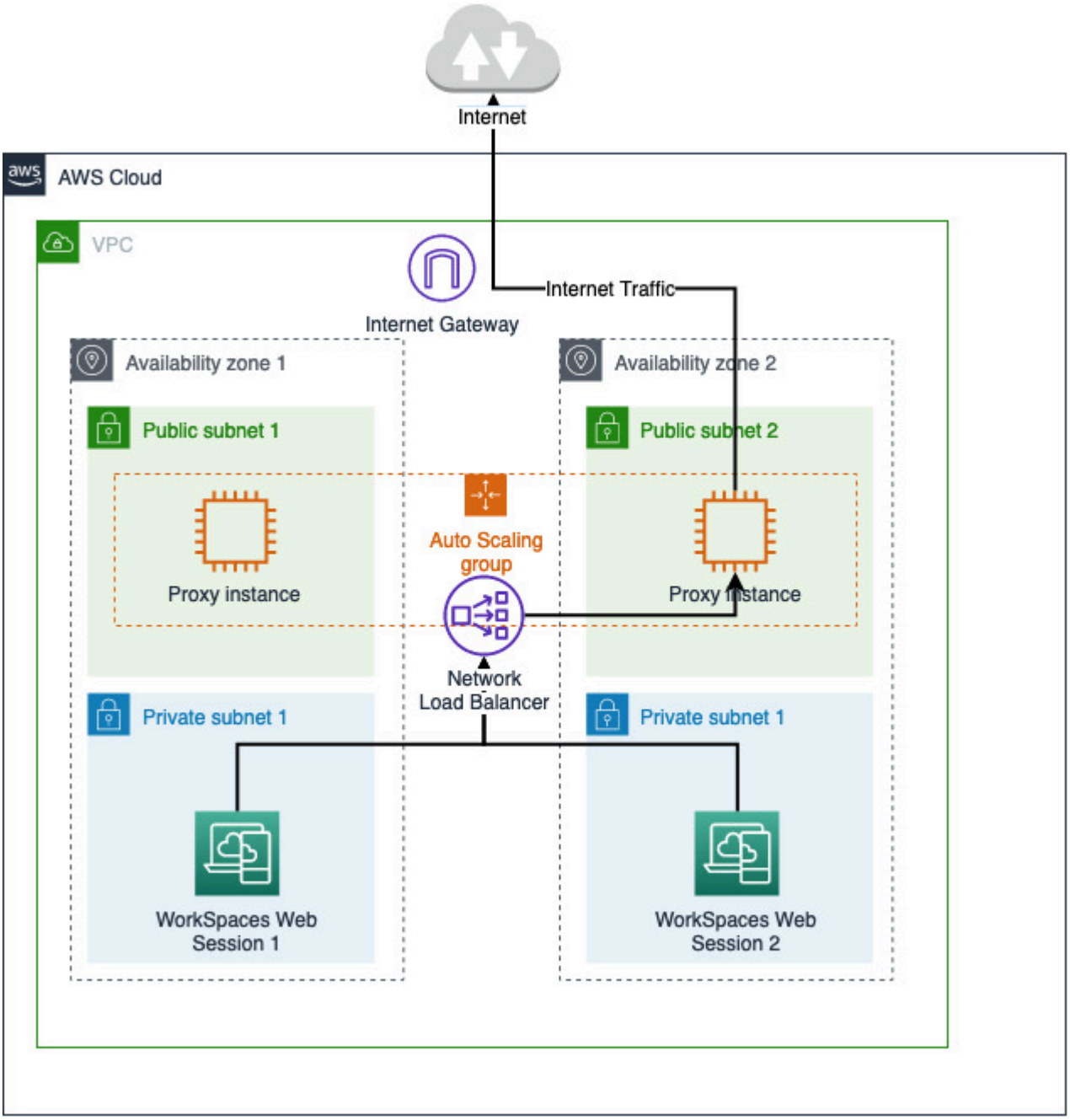
Solusi ini didasarkan pada pengaturan proxy VPC keluar yang direkomendasikan. Solusi proxy didasarkan pada open source HTTP proxy Squid. Kemudian, ia menggunakan pengaturan browser Browser WorkSpaces WorkSpaces Aman untuk mengkonfigurasi portal Browser Aman untuk terhubung ke titik akhir proxy. Untuk informasi selengkapnya, lihat Cara mengatur proxy VPC keluar dengan daftar putih domain dan pemfilteran konten.

Solusi ini memberi Anda manfaat berikut:

- Proxy keluar yang menyertakan grup instans auto-scaling Amazon EC2, yang dihosting oleh penyeimbang beban jaringan. Instans proxy hidup di subnet publik, dan masing-masing terpasang dengan IP Elastis, sehingga mereka dapat memiliki akses ke internet.
- Portal Browser WorkSpaces Aman digunakan untuk subnet pribadi. Anda tidak perlu mengkonfigurasi gateway NAT untuk mengaktifkan akses internet. Sebagai gantinya, Anda mengonfigurasi kebijakan browser Anda, sehingga semua lalu lintas internet melewati proxy keluar. Jika Anda ingin menggunakan proxy Anda sendiri, pengaturan portal Browser WorkSpaces Aman akan serupa.

Arsitektur

Berikut ini adalah contoh pengaturan proxy tipikal di VPC Anda. Instans proxy Amazon EC2 ada di subnet publik dan terkait dengan Elastic IP, sehingga mereka memiliki akses ke internet. Penyeimbang beban jaringan menjadi tuan rumah grup penskalaan otomatis dari instance proxy. Ini memastikan bahwa instance proxy dapat ditingkatkan secara otomatis, dan penyeimbang beban jaringan adalah titik akhir proxy tunggal, yang dapat dikonsumsi oleh sesi Browser WorkSpaces Aman.



Prasyarat

Sebelum memulai, pastikan Anda memenuhi prasyarat berikut:

- Anda memerlukan VPC yang sudah digunakan, dengan subnet publik dan pribadi yang tersebar di beberapa Availability Zone (AZ). Untuk informasi selengkapnya tentang cara mengatur lingkungan VPC, lihat VPC default.

- Anda memerlukan satu titik akhir proxy tunggal yang dapat diakses dari subnet pribadi, tempat sesi Browser WorkSpaces Aman hidup (misalnya, nama DNS penyeimbang beban jaringan). Jika Anda ingin menggunakan proxy yang ada, pastikan juga memiliki satu titik akhir yang dapat diakses dari subnet pribadi Anda.

Siapkan proxy keluar HTTP untuk Browser WorkSpaces Aman

Untuk menyiapkan proxy keluar HTTP untuk Browser WorkSpaces Aman, ikuti langkah-langkah berikut.

1. Untuk menerapkan contoh proksi keluar ke VPC Anda, ikuti langkah-langkah di Cara mengatur proxy VPC keluar dengan daftar putih domain dan pemfilteran konten.
   a. Ikuti langkah-langkah di “Instalasi (pengaturan satu kali)” untuk menyebarkan CloudFormation template ke akun Anda. Pastikan untuk memilih VPC dan subnet yang tepat sebagai parameter template. CloudFormation
   b. Setelah penyebaran, cari parameter CloudFormation output OutboundProxyDomain dan OutboundProxyPort. Ini adalah nama dan port DNS proxy Anda.
   c. Jika Anda sudah memiliki proxy sendiri, lewati langkah ini dan gunakan nama dan port DNS proxy Anda.
2. Di Browser WorkSpaces Aman, konsol, pilih portal Anda dan kemudian pilih Edit.
   a. Dalam detail koneksi Jaringan, pilih VPC dan subnet pribadi yang memiliki akses ke proxy.
   b. Di Pengaturan kebijakan, tambahkan ProxySettings kebijakan berikut menggunakan editor JSON. `ProxyServer`Bidang harus berupa nama dan port DNS proxy Anda. Untuk detail selengkapnya tentang ProxySettings kebijakan, lihat ProxySettings.

```
{
    "chromePolicies":
    {
        ...
        "ProxySettings": {
            "value": {
                "ProxyMode": "fixed_servers",
                "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
                "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
            }
        },
```

```
    }
}
```

3. Dalam sesi Browser WorkSpaces Aman Anda, Anda akan melihat proxy diterapkan ke pengaturan Chrome menggunakan pengaturan proxy dari administrator Anda.
4. Buka chrome: //policy dan tab Kebijakan Chrome untuk mengonfirmasi bahwa kebijakan tersebut diterapkan.
5. Verifikasi bahwa sesi Browser WorkSpaces Aman Anda berhasil menelusuri konten internet tanpa gateway NAT. Di CloudWatch Log, verifikasi bahwa log akses proxy Squid direkam.

Pemecahan Masalah

Setelah kebijakan Chrome diterapkan, jika sesi Browser WorkSpaces Aman Anda masih tidak dapat mengakses internet, ikuti langkah-langkah berikut untuk mencoba menyelesaikan masalah Anda:

- Verifikasi bahwa titik akhir proxy dapat diakses dari subnet pribadi tempat portal Browser WorkSpaces Aman Anda tinggal. Untuk melakukan ini, buat instans EC2 di subnet pribadi, dan uji koneksi dari instans EC2 pribadi ke titik akhir proxy Anda.
- Verifikasi bahwa proxy memiliki akses internet.
- Verifikasi bahwa kebijakan Chrome sudah benar.
  - Konfirmasikan pemformatan berikut untuk `ProxyServer` bidang kebijakan:`<Proxy DNS name>:<Proxy port>`. Seharusnya tidak ada `http://` atau `https://` di awalan.
  - Dalam sesi Browser WorkSpaces Aman, gunakan Chrome untuk menavigasi ke chrome: //policy, dan pastikan ProxySettings kebijakan tersebut berhasil diterapkan.

Rekomendasi pengaturan VPC

Rekomendasi berikut dapat membantu Anda mengonfigurasi VPC Anda dengan lebih efektif dan aman.

Konfigurasi VPC Keseluruhan

- Pastikan konfigurasi VPC Anda dapat mendukung kebutuhan penskalaan Anda.
- Pastikan bahwa kuota layanan Browser WorkSpaces Aman Anda (juga disebut sebagai batas) cukup untuk mendukung permintaan Anda yang diantisipasi. Untuk meminta peningkatan kuota, Anda dapat menggunakan konsol Service Quotas di https://console.aws.amazon.com/

servicequotas/. Untuk informasi tentang kuota Browser WorkSpaces Aman default, lihatthe section called “Kelola kuota layanan untuk portal Anda”.

- Jika Anda berencana untuk menyediakan sesi streaming Anda dengan akses ke internet, kami sarankan Anda mengonfigurasi VPC dengan gateway NAT di subnet publik.

Antarmuka Jaringan Elastis

- Setiap sesi WorkSpaces Secure Browser memerlukan elastic network interface sendiri selama durasi streaming. WorkSpaces Secure Browser menciptakan antarmuka jaringan elastis (ENI) sebanyak kapasitas maksimum yang diinginkan dari armada Anda. Secara default, batas untuk ENI per Wilayah adalah 5000. Untuk informasi selengkapnya, lihat Antarmuka jaringan.

  Saat merencanakan kapasitas untuk penyebaran yang sangat besar, misalnya, ribuan sesi streaming bersamaan, pertimbangkan jumlah ENI yang mungkin diperlukan untuk penggunaan puncak Anda. Kami menyarankan Anda menjaga batas ENI Anda pada atau di atas batas penggunaan bersamaan maksimum yang Anda konfigurasi untuk portal web Anda.

Subnet

- Saat Anda mengembangkan rencana untuk meningkatkan pengguna, ingatlah bahwa setiap sesi Browser WorkSpaces Aman memerlukan alamat IP klien unik dari subnet yang dikonfigurasi. Oleh karena itu, ukuran ruang alamat IP klien yang dikonfigurasi pada subnet Anda menentukan jumlah pengguna yang dapat melakukan streaming secara bersamaan.
- Kami merekomendasikan setiap subnet dikonfigurasi dengan subnet mask yang memungkinkan alamat IP klien yang cukup untuk memperhitungkan jumlah maksimum pengguna bersamaan yang diharapkan. Selain itu, pertimbangkan untuk menambahkan alamat IP tambahan ke akun untuk pertumbuhan yang diantisipasi. Untuk informasi selengkapnya, lihat Ukuran VPC dan Subnet untuk IPv4.
- Kami menyarankan Anda mengonfigurasi subnet di setiap Availability Zone unik yang didukung WorkSpaces Secure Browser di wilayah yang Anda inginkan untuk pertimbangan ketersediaan dan penskalaan. Untuk informasi selengkapnya, lihat the section called “Buat dan konfigurasikan VPC baru”.
- Pastikan bahwa sumber daya jaringan yang diperlukan untuk aplikasi web Anda dapat diakses melalui subnet Anda.

Grup Keamanan

- Gunakan grup keamanan untuk memberikan kontrol akses tambahan ke VPC Anda.

  Grup keamanan yang termasuk dalam VPC Anda memungkinkan Anda mengontrol lalu lintas jaringan antara instance streaming Browser WorkSpaces Aman dan sumber daya jaringan yang diperlukan oleh aplikasi web. Pastikan bahwa grup keamanan menyediakan akses ke sumber daya jaringan yang dibutuhkan aplikasi web Anda.

Zona Ketersediaan yang Didukung

Saat Anda membuat cloud pribadi virtual (VPC) untuk digunakan dengan Browser WorkSpaces Aman, subnet VPC Anda harus berada di Zona Ketersediaan yang berbeda di Wilayah tempat Anda meluncurkan Browser Aman. WorkSpaces Availability Zone berada di lokasi yang berjauhan yang ditata sedemikian rupa agar terisolasi dari kegagalan Availability Zone lain. Dengan meluncurkan instans dalam Availability Zone yang terpisah, Anda dapat melindungi aplikasi Anda dari kegagalan di satu lokasi. Setiap subnet harus berada sepenuhnya dalam satu Availability Zone dan tidak dapat memperluas zona. Sebaiknya konfigurasi subnet untuk setiap AZ yang didukung di wilayah yang Anda inginkan untuk ketahanan maksimum

Availability Zone diwakili oleh kode Wilayah yang diikuti oleh pengidentifikasi huruf; misalnya, `us-east-1a`. Untuk memastikan bahwa sumber daya didistribusikan di seluruh Availability Zone untuk suatu Wilayah, kami secara independen memetakan Availability Zone ke nama untuk setiap akun AWS . Misalnya, Availability Zone `us-east-1a` untuk akun AWS Anda mungkin tidak memiliki lokasi yang sama karena `us-east-1a` untuk akun AWS lainnya.

Untuk mengoordinasikan Availability Zone di seluruh akun, Anda harus menggunakan AZ ID, yang merupakan pengenal unik dan konsisten untuk Availability Zone. Misalnya, `use1-az2` adalah ID AZ untuk `us-east-1` Wilayah dan memiliki lokasi yang sama di setiap AWS akun.

Melihat ID AZ untuk menentukan lokasi sumber daya di satu akun relatif terhadap sumber daya di akun lain. Misalnya, jika Anda membagikan subnet di Availability Zone dengan ID AZ `use1-az2` dengan akun lain, subnet ini tersedia untuk akun tersebut di Availability Zone yang juga memiliki ID AZ yang juga `use1-az2`. ID AZ untuk setiap VPC dan subnet ditampilkan di konsol Amazon VPC.

WorkSpaces Browser Aman tersedia dalam subset Availability Zones untuk setiap Wilayah yang didukung. Tabel berikut mencantumkan ID AZ yang dapat Anda gunakan untuk setiap Wilayah. Untuk melihat pemetaan ID AZ ke Availability Zone di akun Anda, lihat ID AZ untuk Sumber Daya Anda di AWS RAM Panduan Pengguna.

Nama Wilayah	Kode Wilayah	ID AZ yang didukung
US East (N. Virginia)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
US West (Oregon)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Asia Pasifik (Mumbai)	ap-south-1	aps1-az1, aps1-az3
Asia Pasifik (Seoul)	ap-northeast-2	apne2-az1 , apne2-az2 , apne2-az3
Asia Pasifik (Singapura)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
Asia Pasifik (Sydney)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
Asia Pasifik (Tokyo)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
Kanada (Pusat)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
Eropa (Frankfurt)	eu-central-1	euc1-az2, euc1-az2, euc1-az3
Eropa (Irlandia)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Eropa (London)	eu-west-2	euw2-az1, euw2-az2

Untuk informasi selengkapnya tentang Availability Zone dan AZ ID, lihat Wilayah, Availability Zone, dan Local Zones di Panduan Pengguna Amazon EC2.

Koneksi VPC

Setiap instance streaming Browser WorkSpaces Aman memiliki antarmuka jaringan pelanggan yang menyediakan konektivitas ke sumber daya dalam VPC Anda, serta ke internet jika subnet pribadi dengan gateway NAT diatur.

Untuk konektivitas internet, port berikut harus terbuka untuk semua tujuan. Jika Anda menggunakan grup keamanan yang dimodifikasi atau kustom, Anda harus menambahkan aturan yang diperlukan secara manual. Untuk informasi selengkapnya, lihat Aturan grup keamanan.

> **Note**
>
> Ini berlaku untuk lalu lintas jalan keluar.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8433

Koneksi klien/pengguna

WorkSpaces Browser Aman dikonfigurasi untuk merutekan koneksi streaming melalui internet publik. Konektivitas internet diperlukan untuk mengautentikasi pengguna dan mengirimkan aset web yang dibutuhkan WorkSpaces Secure Browser agar berfungsi. Untuk mengizinkan lalu lintas ini, Anda harus mengizinkan domain yang tercantum di dalamnyaDomain yang diizinkan.

Topik berikut memberikan informasi tentang cara mengaktifkan koneksi pengguna ke Browser WorkSpaces Aman.

Topik

- Alamat IP dan persyaratan port
- Domain yang diizinkan

Alamat IP dan persyaratan port

Untuk mengakses instance Browser WorkSpaces Aman, perangkat pengguna memerlukan akses keluar pada port berikut:

- Port 443 (TCP)
  - Port 443 digunakan untuk komunikasi HTTPS antara perangkat pengguna dan instance streaming saat menggunakan titik akhir internet. Biasanya, ketika pengguna akhir menjelajah web selama sesi streaming, browser web secara acak memilih port sumber dalam kisaran tinggi untuk lalu lintas streaming. Anda harus memastikan bahwa lalu lintas kembali ke port ini diizinkan.
  - Port ini harus terbuka untuk domain yang diperlukan yang tercantum diDomain yang diizinkan.
  - AWS menerbitkan rentang alamat IP saat ini, termasuk rentang yang dapat diselesaikan oleh Session Gateway dan CloudFront domain, dalam format JSON. Untuk informasi tentang cara mengunduh file.json dan melihat rentang saat ini, lihat rentang alamat AWS IP. Atau, jika Anda menggunakan AWS Tools for Windows PowerShell, Anda dapat mengakses informasi yang sama dengan menggunakan Get-AWSPublicIpAddressRange PowerShell perintah. Untuk informasi selengkapnya, lihat Menanyakan Rentang Alamat IP Publik untuk AWS.
- (Opsional) Port 53 (UDP)
  - Port 53 digunakan untuk komunikasi antara perangkat pengguna dan server DNS Anda.
  - Port ini opsional jika Anda tidak menggunakan server DNS untuk resolusi nama domain.
  - Port harus terbuka ke alamat IP untuk server DNS Anda sehingga nama domain publik dapat diselesaikan.

Domain yang diizinkan

Agar pengguna dapat mengakses portal web dari browser lokal mereka, Anda harus menambahkan domain berikut ke daftar izinkan di jaringan tempat pengguna mencoba mengakses layanan tersebut.

Pada tabel berikut, ganti *{region}* dengan kode Region portal web operasi. Misalnya, s3. *{region}* .amazonaws.com harus s3.eu-west-1.amazonaws.com untuk portal web wilayah Eropa (Irlandia). Untuk daftar kode Wilayah, lihat titik akhir dan kuota Amazon WorkSpaces Secure Browser.

Kategori	Domain atau Alamat IP
WorkSpaces Aset streaming Browser yang aman	s3. *{wilayah} .amazonaws.com* s3.amazonaws.com

Kategori	Domain atau Alamat IP
	appstream2. *{wilayah}* *.aws.amazon.com* *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Amankan aset statis Browser	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Otentikasi Browser Aman	*.auth. *{wilayah}* .amazoncognito.com kognito-identitas. *{wilayah}* *.amazonaws.com* kognito-idp. *{wilayah}* *.amazonaws.com* *.cloudfront.net
WorkSpaces Metrik dan pelaporan Browser yang aman	*.eksekusi api. *{wilayah}* *.amazonaws.com* unagi-id.amazon.com

Bergantung pada penyedia identitas yang dikonfigurasi, Anda mungkin juga perlu mengizinkan daftar domain tambahan. Tinjau dokumentasi IDP Anda untuk mengidentifikasi domain mana yang Anda perlukan untuk mengizinkan daftar agar Browser WorkSpaces Aman dapat menggunakan penyedia tersebut. Jika Anda menggunakan Pusat Identitas IAM, lihat prasyarat Pusat Identitas IAM untuk informasi lebih lanjut.

Memulai dengan Browser WorkSpaces Aman

Ikuti langkah-langkah ini untuk membuat portal web Browser WorkSpaces Aman dan memberi pengguna akses ke situs web internal dan SaaS dari browser yang ada. Anda dapat membuat satu portal web di setiap wilayah yang didukung per akun.

> **Note**
>
> Untuk meminta peningkatan batas untuk lebih dari satu portal, silakan hubungi dukungan dengan Akun AWS ID Anda, jumlah portal yang akan diminta, dan Wilayah AWS.

Proses ini biasanya memakan waktu lima menit dengan wizard pembuatan portal web, dan hingga 15 menit tambahan agar portal menjadi Aktif.

Tidak ada biaya yang terkait dengan pengaturan portal web. WorkSpaces Secure Browser menawarkan pay-as-you-go harga, termasuk harga bulanan yang rendah untuk pengguna yang secara aktif menggunakan layanan ini. Tidak ada biaya di muka, lisensi, atau komitmen jangka panjang.

> **Important**
>
> Sebelum Anda mulai, Anda harus menyelesaikan prasyarat yang diperlukan untuk portal web. Untuk informasi lebih lanjut tentang prasyarat portal web, lihat. Menyiapkan Browser WorkSpaces Aman

Topik

- Langkah 1: Buat portal web
- Langkah 2: Uji portal web Anda
- Langkah 3: Mendistribusikan portal web Anda
- Langkah selanjutnya

Langkah 1: Buat portal web

Ikuti langkah-langkah ini untuk membuat portal web.

Topik

- Konfigurasikan pengaturan jaringan
- Konfigurasikan pengaturan portal
- Konfigurasikan pengaturan pengguna
- Konfigurasikan penyedia identitas
- Tinjau dan luncurkan

Konfigurasikan pengaturan jaringan

1. Buka konsol Browser WorkSpaces Aman di https://console.aws.amazon.com/workspaces-web/home.
2. Pilih Browser WorkSpaces Aman, lalu portal Web, lalu pilih Buat portal web.
3. Pada Langkah 1: Tentukan halaman koneksi jaringan, selesaikan langkah-langkah berikut untuk menghubungkan VPC Anda ke portal web Anda dan konfigurasikan VPC dan subnet Anda.
    1. Untuk detail Jaringan, pilih VPC dengan koneksi ke konten yang ingin diakses pengguna dengan WorkSpaces Secure Browser.
    2. Pilih hingga tiga subnet pribadi yang memenuhi persyaratan berikut. Untuk informasi selengkapnya, lihat Jaringan dan akses.
        - Anda harus memilih minimal dua subnet pribadi untuk membuat portal.
        - Untuk memastikan ketersediaan yang tinggi untuk portal web Anda, kami sarankan Anda menyediakan jumlah maksimum subnet pribadi di zona ketersediaan unik untuk VPC Anda.
    3. Pilih grup keamanan.

Konfigurasikan pengaturan portal

Pada Langkah 2: Konfigurasikan halaman pengaturan portal web, selesaikan langkah-langkah berikut untuk menyesuaikan pengalaman penjelajahan pengguna Anda saat mereka memulai sesi.

1. Di bawah detail portal Web, untuk nama Tampilan, masukkan nama yang dapat diidentifikasi untuk portal web Anda.
2. Di bawah Jenis Instance, pilih jenis instans untuk portal web Anda dari menu tarik-turun. Kemudian, masukkan batas pengguna bersamaan Max Anda untuk portal web. Untuk informasi selengkapnya, lihat the section called “Kelola kuota layanan untuk portal Anda”.

> **Note**
>
> Memilih jenis instans baru akan mengubah biaya untuk setiap pengguna aktif bulanan. Untuk informasi selengkapnya, lihat Harga Amazon WorkSpaces Secure Browser.

3. Di bawah Pencatatan akses pengguna, untuk ID aliran Kinesis, pilih aliran data Amazon Kinesis yang ingin Anda kirimi datanya. Untuk informasi selengkapnya, lihat the section called “Siapkan pencatatan akses pengguna”.
4. Di bawah Pengaturan kebijakan, selesaikan yang berikut ini:

   - Untuk opsi Kebijakan, pilih Editor visual atau unggahan file JSON. Anda dapat menggunakan salah satu metode untuk memberikan detail konfigurasi kebijakan untuk portal web Anda. Untuk informasi selengkapnya, lihat the section called “Menyetel atau mengedit kebijakan browser”.
     - WorkSpaces Browser Aman mencakup dukungan untuk kebijakan perusahaan Chrome. Anda dapat menambahkan dan mengelola kebijakan dengan editor visual atau unggahan manual untuk file kebijakan. Anda dapat beralih di antara salah satu opsi kapan saja.
     - Saat mengunggah file kebijakan, Anda dapat melihat kebijakan yang tersedia di file di konsol. Namun, Anda tidak dapat mengedit semua kebijakan di editor visual. Konsol mencantumkan kebijakan dalam file JSON yang tidak dapat Anda edit dengan editor visual di bawah kebijakan JSON Tambahan. Untuk membuat perubahan pada kebijakan ini, Anda harus mengeditnya secara manual.
   - (Opsional) Untuk URL Startup - opsional, masukkan domain untuk digunakan sebagai beranda saat pengguna meluncurkan browser mereka. VPC Anda harus memiliki koneksi yang stabil ke URL ini.
   - Pilih atau hapus Penjelajahan pribadi dan penghapusan Riwayat untuk mengaktifkan atau menonaktifkan fitur ini selama sesi pengguna

   > **Note**
   >
   > URL yang dikunjungi saat menjelajah secara pribadi, atau sebelum pengguna menghapus riwayat browser mereka, tidak dapat direkam dalam pencatatan akses pengguna. Untuk informasi selengkapnya, lihat the section called “Siapkan pencatatan akses pengguna”.

- Di bawah pemfilteran URL, Anda dapat mengonfigurasi URL mana yang dapat dikunjungi pengguna selama sesi. Untuk informasi selengkapnya, lihat the section called “Mengatur pemfilteran URL”.
- (Opsional) Untuk bookmark Browser - opsional, masukkan nama Tampilan, Domain, dan Folder untuk setiap bookmark yang Anda ingin pengguna Anda lihat di browser mereka. Kemudian, pilih Tambahkan bookmark.

  > **Note**
  >
  > Domain adalah bidang wajib untuk bookmark browser.
  > Di Chrome, pengguna dapat menemukan bookmark terkelola di folder Bookmark terkelola pada bilah alat bookmark.

- (Opsional) Tambahkan Tag ke portal Anda. Anda dapat menggunakan tag untuk mencari atau memfilter AWS sumber daya Anda. Tag terdiri dari kunci dan nilai opsional dan dikaitkan dengan sumber daya portal Anda.

5. Di bawah Kontrol Akses IP (opsional), pilih apakah akan membatasi akses ke jaringan tepercaya. Untuk informasi selengkapnya, lihat the section called “Mengatur kontrol akses IP (opsional)”.
6. Pilih Next untuk melanjutkan.

Konfigurasikan pengaturan pengguna

Pada Langkah 3: Pilih halaman pengaturan pengguna, selesaikan langkah-langkah berikut untuk memilih fitur mana yang dapat diakses pengguna Anda dari bilah navigasi atas selama sesi mereka, lalu pilih Berikutnya:

1. Untuk izin Pengguna, pilih apakah akan mengaktifkan ekstensi untuk sistem masuk tunggal. Untuk informasi selengkapnya, lihat the section called “Aktifkan ekstensi untuk sistem masuk tunggal (opsional)”.
2. Untuk izin Clipboard, pilih Dinonaktifkan atau Diaktifkan.
3. Di bawah Transfer file, pilih Dinonaktifkan atau Diaktifkan.
4. Untuk Izinkan pengguna mencetak ke perangkat lokal dari portal web mereka, pilih Diizinkan atau Tidak diizinkan.

5. Untuk Izinkan pengguna melakukan deeplink ke portal web mereka, pilih Diizinkan atau Tidak Diizinkan. Untuk informasi lebih lanjut tentang deep link, lihatthe section called “Izinkan tautan dalam (opsional)”.
6. Untuk detail sesi Pengguna, tentukan yang berikut ini:

   - Untuk Putuskan batas waktu dalam hitungan menit, pilih jumlah waktu sesi streaming tetap aktif setelah pengguna memutuskan sambungan. Jika pengguna mencoba menyambung kembali ke sesi streaming setelah pemutusan atau gangguan jaringan dalam interval waktu ini, mereka terhubung ke sesi sebelumnya. Jika tidak, mereka terhubung ke sesi baru dengan instans streaming baru.

     Jika pengguna mengakhiri sesi, batas waktu pemutusan tidak berlaku. Sebagai gantinya, pengguna diminta untuk menyimpan dokumen yang terbuka, dan kemudian segera terputus dari instance streaming. Contoh yang digunakan pengguna kemudian dihentikan.
   - Untuk batas waktu pemutusan Idle dalam hitungan menit, pilih jumlah waktu pengguna dapat menganggur (tidak aktif) sebelum mereka terputus dari sesi streaming mereka dan batas waktu Putuskan sambungan dalam interval waktu menit dimulai. Pengguna diberi tahu sebelum mereka terputus karena tidak aktif. Jika mereka mencoba menyambung kembali ke sesi streaming sebelum interval waktu yang ditentukan dalam batas waktu Putuskan sambungan dalam menit telah berlalu, mereka terhubung ke sesi sebelumnya. Jika tidak, mereka terhubung ke sesi baru dengan instans streaming baru. Menyetel nilai ini ke 0 menonaktifkannya. Ketika nilai ini dinonaktifkan, pengguna tidak terputus karena tidak aktif.

     > **Note**
     >
     > Pengguna dianggap dalam keadaan diam ketika mereka berhenti memberikan input keyboard atau mouse selama sesi streaming mereka. Unggahan dan unduhan file, audio masuk, audio keluar, dan perubahan piksel tidak memenuhi syarat sebagai aktivitas pengguna. Jika pengguna terus menganggur setelah interval waktu di batas waktu pemutusan Idle dalam beberapa menit berlalu, mereka terputus.

Konfigurasikan penyedia identitas

Gunakan langkah-langkah berikut untuk mengonfigurasi penyedia identitas Anda (iDP).

Topik

- Pilih jenis penyedia identitas
- Konfigurasikan jenis otentikasi standar
- Konfigurasikan jenis autentikasi Pusat Identitas IAM
- Mengubah tipe penyedia identitas

Pilih jenis penyedia identitas

WorkSpaces Secure Browser menawarkan dua jenis otentikasi: Standar dan AWS IAM Identity Center. Anda memilih jenis otentikasi yang akan digunakan dengan portal Anda di halaman Konfigurasi penyedia identitas.

- Untuk Standar (opsi default), gabungkan penyedia identitas SAMP 2.0 pihak ketiga Anda (seperti Okta atau Ping) langsung dengan portal Anda. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan jenis otentikasi standar”. Tipe standar mendukung alur otentikasi yang diprakarsai SP dan yang diprakarsai IDP.
- Untuk Pusat Identitas IAM (opsi lanjutan), gabungkan Pusat Identitas IAM dengan portal Anda. Untuk menggunakan jenis otentikasi ini, Pusat Identitas IAM dan portal Browser WorkSpaces Aman Anda harus berada di tempat yang sama. Wilayah AWS Untuk informasi selengkapnya, lihat the section called “Konfigurasikan jenis autentikasi Pusat Identitas IAM”.

Konfigurasikan jenis otentikasi standar

Untuk Standar (default), gabungkan penyedia identitas SAMP 2.0 pihak ketiga Anda (seperti Okta atau Ping) langsung dengan portal Anda.

Tipe identitas Standar dapat mendukung alur masuk service-provider-initiated (dimulai SP) dan identity-provider-initiated (diprakarsai IDP) dengan IDP yang sesuai dengan SAMP 2.0 Anda.

Langkah 1: Mulai mengkonfigurasi penyedia identitas Anda di Browser WorkSpaces Aman

Selesaikan langkah-langkah berikut untuk mengonfigurasi penyedia identitas Anda:

1. Pada halaman Configure identity provider dari wizard pembuatan, pilih Standard.
2. Pilih Lanjutkan dengan IDP Standar.
3. Unduh file metadata SP, dan biarkan tab tetap terbuka untuk nilai metadata individual.

- Jika file metadata SP tersedia, pilih Unduh file metadata untuk mengunduh dokumen metadata penyedia layanan (SP), dan unggah file metadata penyedia layanan ke IDP Anda di langkah berikutnya. Tanpa ini, pengguna tidak akan dapat masuk.
- Jika penyedia Anda tidak mengunggah file metadata SP, masukkan nilai metadata secara manual.

4. Di bawah Pilih tipe login SAMP, pilih antara pernyataan SAMP yang diprakarsai SP dan yang diprakarsai IDP, atau hanya pernyataan SAMP yang diprakarsai SP.

- Pernyataan SAMP yang diprakarsai SP dan yang diprakarsai IDP memungkinkan portal Anda mendukung kedua jenis alur masuk. Portal yang mendukung alur yang diprakarsai IDP memungkinkan Anda menyajikan pernyataan SAMP ke titik akhir federasi identitas layanan tanpa mengharuskan pengguna untuk meluncurkan sesi dengan mengunjungi URL portal.
  - Pilih ini untuk memungkinkan portal menerima pernyataan SAMP yang diprakarsai IDP yang tidak diminta.
  - Opsi ini memerlukan Status Relay default untuk dikonfigurasi di Penyedia Identitas SAMP 2.0 Anda. Parameter status Relay untuk portal Anda ada di konsol di bawah login SAMP yang dimulai IDP, atau Anda dapat menyalinnya dari file metadata SP di bawah. `<md:IdPInitRelayState>`
  - Catatan
    - Berikut ini adalah format status relai:`redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex` `Identity-Provider`.
    - Jika Anda menyalin dan menempelkan nilai dari file metadata SP, pastikan Anda mengubahnya`&` . & `&`adalah karakter pelarian XHTML.
- Pilih pernyataan SAMP yang diprakarsai SP hanya agar portal hanya mendukung alur masuk yang dimulai SP. Opsi ini akan menolak pernyataan SAMP yang tidak diminta dari alur masuk yang diprakarsai IDP.

> **Note**
>
> Beberapa pihak ketiga IdPs memungkinkan Anda membuat aplikasi SAMP khusus yang dapat memberikan pengalaman otentikasi yang diprakarsai IDP dengan memanfaatkan alur yang diprakarsai SP. Misalnya, lihat Menambahkan aplikasi bookmark Okta.

5. Pilih apakah Anda ingin mengaktifkan permintaan Tanda tangani SAMP ke penyedia ini. Otentikasi yang dimulai SP memungkinkan IDP Anda untuk memvalidasi bahwa permintaan otentikasi berasal dari portal, yang mencegah penerimaan permintaan pihak ketiga lainnya.
   a. Unduh sertifikat penandatanganan dan unggah ke IDP Anda. Sertifikat penandatanganan yang sama dapat digunakan untuk logout tunggal.
   b. Aktifkan permintaan yang ditandatangani di IDP Anda. Namanya mungkin berbeda, tergantung pada IDP.

   > **Note**
   >
   > RSA-SHA256 adalah satu-satunya permintaan dan algoritma penandatanganan permintaan default yang didukung.

6. Pilih apakah Anda ingin mengaktifkan Perlukan pernyataan SAMP terenkripsi. Ini memungkinkan Anda untuk mengenkripsi pernyataan SAMP yang berasal dari IDP Anda. Hal ini dapat mencegah data dari dicegat dalam pernyataan SAMP antara IDP dan Secure Browser. WorkSpaces

   > **Note**
   >
   > Sertifikat enkripsi tidak tersedia pada langkah ini. Ini akan dibuat setelah portal Anda diluncurkan. Setelah Anda meluncurkan portal, unduh sertifikat enkripsi dan unggah ke IDP Anda. Kemudian, aktifkan enkripsi pernyataan di IDP Anda (namanya mungkin berbeda, tergantung pada IDP.

7. Pilih apakah Anda ingin mengaktifkan Single Logout. Single logout memungkinkan pengguna akhir Anda untuk keluar dari sesi IDP WorkSpaces dan Secure Browser mereka dengan satu tindakan.
   a. Unduh sertifikat penandatanganan dari WorkSpaces Secure Browser dan unggah ke IDP Anda. Ini adalah sertifikat penandatanganan yang sama yang digunakan untuk Penandatanganan Permintaan pada langkah sebelumnya.
   b. Menggunakan Single Logout mengharuskan Anda untuk mengonfigurasi URL Logout Tunggal di penyedia identitas SAMP 2.0 Anda. Anda dapat menemukan URL Logout Tunggal untuk portal Anda di konsol di bawah Detail penyedia layanan (SP) - Tampilkan nilai metadata individual, atau dari file metadata SP di bawah. `<md:SingleLogoutService>`
   c. Aktifkan Single Logout di IDP Anda. Namanya mungkin berbeda, tergantung pada IDP.

Langkah 2: Konfigurasikan penyedia identitas Anda di IDP Anda sendiri

Buka tab baru di browser Anda. Kemudian, selesaikan langkah-langkah berikut dengan IDP Anda:

1. Tambahkan metadata portal Anda ke IDP SAMP Anda.

   Unggah dokumen metadata SP yang Anda unduh di langkah sebelumnya ke iDP Anda, atau salin dan tempel nilai metadata ke bidang yang benar di iDP Anda. Beberapa penyedia tidak mengizinkan pengunggahan file.

   Rincian proses ini dapat bervariasi antar penyedia. Temukan dokumentasi penyedia Anda the section called “Panduan untuk spesifik IdPs” untuk mendapatkan bantuan tentang cara menambahkan detail portal ke konfigurasi IDP Anda.
2. Konfirmasikan NameID untuk pernyataan SAMP Anda.

   Pastikan IDP SAMP Anda mengisi nameID di pernyataan SAMP dengan bidang email pengguna. NameID dan email pengguna digunakan untuk mengidentifikasi pengguna federasi SAMP Anda secara unik dengan portal. Gunakan format ID Nama SAMP persisten.
3. Opsional: Konfigurasikan Status Relay untuk otentikasi yang diprakarsai IDP.

   Jika Anda memilih Accept SP-initiated dan IDP-initiated SAMP assertions pada langkah sebelumnya, ikuti langkah-langkah di langkah 2 untuk the section called “Langkah 1: Mulai mengkonfigurasi penyedia identitas Anda di Browser WorkSpaces Aman” mengatur Status Relay default untuk aplikasi IDP Anda.
4. Opsional: Konfigurasikan penandatanganan Permintaan. Jika Anda memilih Menandatangani permintaan SAMP ke penyedia ini pada langkah sebelumnya, ikuti langkah-langkah di langkah 3 the section called “Langkah 1: Mulai mengkonfigurasi penyedia identitas Anda di Browser WorkSpaces Aman” untuk mengunggah sertifikat penandatanganan ke IDP Anda dan mengaktifkan penandatanganan permintaan. Beberapa IdPs seperti Okta mungkin mengharuskan NameID Anda termasuk dalam tipe “persisten” untuk menggunakan penandatanganan Permintaan. Pastikan untuk mengonfirmasi NameID Anda untuk pernyataan SAMP Anda dengan mengikuti langkah-langkah di atas.
5. Opsional: Konfigurasikan enkripsi Assertion. Jika Anda memilih Memerlukan pernyataan SAMP terenkripsi dari penyedia ini, tunggu hingga pembuatan portal selesai, lalu ikuti langkah 4 di “Unggah metadata” di bawah ini untuk mengunggah sertifikat enkripsi ke IDP Anda dan mengaktifkan enkripsi pernyataan.
6. Opsional: Konfigurasikan Single Logout. Jika Anda memilih Single Logout, ikuti langkah-langkah di langkah 5 the section called “Langkah 1: Mulai mengkonfigurasi penyedia identitas Anda di

Browser WorkSpaces Aman" untuk mengunggah sertifikat penandatanganan ke IDP Anda, isi URL Logout Tunggal, dan aktifkan Single Logout.

7. Berikan akses ke pengguna Anda di IDP Anda untuk menggunakan Browser WorkSpaces Aman.
8. Unduh file pertukaran metadata dari IDP Anda. Anda akan mengunggah metadata ini ke WorkSpaces Secure Browser di langkah berikutnya.

Langkah 3: Selesai mengonfigurasi penyedia identitas Anda di Browser WorkSpaces Aman

Kembali ke WorkSpaces Secure Browserconsole. Pada halaman Konfigurasi penyedia identitas dari panduan pembuatan, di bawah metadata iDP, unggah file metadata, atau masukkan URL metadata dari iDP Anda. Portal menggunakan metadata ini dari IDP Anda untuk membangun kepercayaan.

1. Untuk mengunggah file metadata, di bawah dokumen metadata iDP, pilih Pilih file. Unggah file metadata berformat XML dari IDP yang Anda unduh pada langkah sebelumnya.
2. Untuk menggunakan URL metadata, buka IDP yang Anda atur pada langkah sebelumnya dan dapatkan URL Metadata-nya. Kembali ke konsol Browser WorkSpaces Aman, dan di bawah URL metadata iDP, masukkan url metadata yang Anda peroleh dari iDP Anda.
3. Setelah selesai, pilih Berikutnya.
4. Untuk portal di mana Anda telah mengaktifkan Perlukan pernyataan SAMP terenkripsi dari opsi penyedia ini, Anda perlu mengunduh sertifikat enkripsi dari bagian detail iDP portal dan mengunggahnya ke IDP Anda. Kemudian, Anda dapat mengaktifkan opsi di sana.

> **Note**
>
> WorkSpaces Browser Aman memerlukan subjek atau nameID untuk dipetakan dan disetel dalam pernyataan SAMP dalam pengaturan IDP Anda. IDP Anda dapat membuat pemetaan ini secara otomatis. Jika pemetaan ini tidak dikonfigurasi dengan benar, pengguna Anda tidak dapat masuk ke portal web dan memulai sesi.
> WorkSpaces Browser Aman mengharuskan klaim berikut hadir dalam respons SAMP. Anda dapat menemukan <Your SP Entity ID>dan <Your SP ACS URL>dari detail penyedia layanan portal atau dokumen metadata Anda, baik melalui konsol atau CLI.
>
> - `AudienceRestriction`Klaim dengan `Audience` nilai yang menetapkan ID Entitas SP Anda sebagai target respons. Contoh:
>
> ```
> <saml:AudienceRestriction>
>     <saml:Audience><Your SP Entity ID></saml:Audience>
> ```

```
</saml:AudienceRestriction>
```

- `ResponseKlaim` dengan `InResponseTo` nilai ID permintaan SAMP asli. Contoh:

```
<samlp:Response ... InResponseTo="<originalSAMLrequestId>">
```

- `SubjectConfirmationDataKlaim` dengan `Recipient` nilai URL SP ACS Anda, dan `InResponseTo` nilai yang cocok dengan ID permintaan SAMP asli. Contoh:

```
<saml:SubjectConfirmation>
    <saml:SubjectConfirmationData ...
        Recipient="<Your SP ACS URL>"
        InResponseTo="<originalSAMLrequestId>"
        />
</saml:SubjectConfirmation>
```

WorkSpaces Browser Aman memvalidasi parameter permintaan dan pernyataan SAMP Anda. Untuk pernyataan SAMP yang diprakarsai IDP, rincian permintaan Anda harus diformat sebagai `RelayState` parameter di badan permintaan HTTP POST. Badan permintaan juga harus berisi pernyataan SAMP Anda sebagai parameter. `SAMLResponse` Keduanya harus ada jika Anda telah mengikuti langkah sebelumnya.
Berikut ini adalah contoh `POST` badan untuk penyedia SAMP yang diprakarsai IDP.

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

Panduan untuk spesifik IdPs

Untuk memastikan Anda mengonfigurasi federasi SAMP dengan benar untuk portal Anda, lihat tautan di bawah ini untuk dokumentasi dari yang umum digunakan IdPs.

IdP	Pengaturan aplikasi SAMP	Manajemen pengguna	Autentikasi yang diprakarsai IDP	Permintaan penandatanganan	Enkripsi pernyataan	Keluar tunggal
Okta	Buat integrasi	Manajemen pengguna	Referensi bidang Wizard	Referensi bidang Wizard	Referensi bidang Wizard	Referensi bidang Wizard

IdP	Pengaturan aplikasi SAMP	Manajemen pengguna	Autentikasi yang diprakarsai IDP	Permintaan penandatanganan	Enkripsi pernyataan	Keluar tunggal
	aplikasi SAMP		Integrasi Aplikasi SAMP	Integrasi Aplikasi SAMP	Integrasi Aplikasi SAMP	Integrasi Aplikasi SAMP
Entra	Buat aplikasi Anda sendiri	Mulai cepat: Buat dan tetapkan akun pengguna	Aktifkan sistem masuk tunggal untuk aplikasi perusahaan	SAMP Minta Verifikasi Tanda Tangan	Konfigurasikan enkripsi token Microsoft Entra SAMP	Protokol SAMP Keluar Tunggal
Ping	Tambahkan aplikasi SAMP	Pengguna	Mengaktifkan SSO yang diprakarsai IDP	Mengkonfigurasi permintaan otentikasi masuk untuk Enterprise PingOne	Apakah PingOne untuk Enterprise mendukung enkripsi?	SAMP 2.0 logout tunggal
Satu Login	Konektor Kustom SAMP (Lanjutan) (4266907)	Tambahkan Pengguna ke OneLogin Secara Manual	Konektor Kustom SAMP (Lanjutan) (4266907)	Konektor Kustom SAMP (Lanjutan) (4266907)	Konektor Kustom SAMP (Lanjutan) (4266907)	Konektor Kustom SAMP (Lanjutan) (4266907)

IdP	Pengaturan aplikasi SAMP	Manajemen pengguna	Autentikasi yang diprakarsai IDP	Permintaan penandatanganan	Enkripsi pernyataan	Keluar tunggal
Pusat Identitas IAM	Siapkan aplikasi SAMP 2.0 Anda sendiri	Siapkan aplikasi SAMP 2.0 Anda sendiri	Siapkan aplikasi SAMP 2.0 Anda sendiri	N/A	N/A	N/A

Konfigurasikan jenis autentikasi Pusat Identitas IAM

Untuk tipe Pusat Identitas IAM (lanjutan), Anda menggabungkan Pusat Identitas IAM dengan portal Anda. Hanya pilih opsi ini jika hal berikut berlaku untuk Anda:

- Pusat Identitas IAM Anda dikonfigurasi dalam hal yang sama Akun AWS dan Wilayah AWS sebagai portal web Anda.
- Jika Anda menggunakan AWS Organizations, Anda menggunakan akun manajemen.

Sebelum membuat portal web dengan tipe autentikasi IAM Identity Center, Anda harus menyiapkan IAM Identity Center sebagai penyedia mandiri. Untuk informasi selengkapnya, lihat Memulai tugas umum di Pusat Identitas IAM. Atau, Anda dapat menghubungkan SAMP 2.0 IDP Anda ke IAM Identity Center. Untuk informasi selengkapnya, lihat Connect ke penyedia identitas eksternal. Jika tidak, Anda tidak akan memiliki pengguna atau grup untuk ditetapkan ke portal web Anda.

Jika Anda sudah menggunakan IAM Identity Center, Anda dapat memilih IAM Identity Center sebagai jenis penyedia dan ikuti langkah-langkah di bawah ini untuk menambah, melihat, atau menghapus pengguna atau grup dari portal web Anda.

> **Note**
>
> Untuk menggunakan jenis otentikasi ini, Pusat Identitas IAM Anda harus sama Akun AWS dan Wilayah AWS sebagai portal Browser WorkSpaces Aman Anda. Jika Pusat Identitas IAM Anda terpisah Akun AWS atau Wilayah AWS, ikuti petunjuk untuk jenis otentikasi Standar. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan jenis otentikasi standar”.

Jika Anda menggunakan AWS Organizations, Anda hanya dapat membuat portal Browser WorkSpaces Aman yang terintegrasi dengan IAM Identity Center menggunakan akun manajemen.

Untuk membuat portal web dengan IAM Identity Center

1. Selama pembuatan portal pada Langkah 4: Konfigurasikan penyedia identitas, pilih AWS IAM Identity Center.
2. Pilih Lanjutkan dengan Pusat Identitas IAM.
3. Pada halaman Tetapkan pengguna dan grup, pilih tab Pengguna dan/atau Grup.
4. Centang kotak di samping pengguna atau grup yang ingin Anda tambahkan ke portal.
5. Setelah Anda membuat portal, pengguna yang terkait dapat masuk ke Browser WorkSpaces Aman dengan nama pengguna dan kata sandi Pusat Identitas IAM mereka.

Untuk mengelola portal web Anda dengan IAM Identity Center

1. Setelah Anda membuat portal Anda, itu terdaftar di konsol Pusat Identitas IAM sebagai aplikasi yang dikonfigurasi.
2. Untuk mengakses konfigurasi aplikasi ini, pilih Aplikasi di sidebar, dan cari aplikasi yang dikonfigurasi dengan nama yang cocok dengan nama tampilan untuk portal web Anda.

> **Note**
>
> Jika Anda belum memasukkan nama tampilan, GUID portal Anda ditampilkan sebagai gantinya. GUID adalah ID yang diawali dengan URL endpoint portal web Anda.

Untuk menambahkan pengguna dan grup tambahan ke portal web yang ada

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Edit.
3. Pilih Pengaturan penyedia identitas dan Tetapkan pengguna dan grup tambahan. Dari sini, Anda dapat menambahkan pengguna dan grup ke portal web Anda.

> **Note**
>
> Anda tidak dapat menambahkan pengguna atau grup dari konsol Pusat Identitas IAM. Anda harus melakukan ini dari halaman edit portal Browser WorkSpaces Aman Anda.

Untuk melihat atau menghapus pengguna dan grup untuk portal web Anda

- Anda dapat melihat atau menghapus akses pengguna ke aplikasi ini dengan menggunakan tindakan yang tersedia di tabel Pengguna yang Ditugaskan. Untuk informasi selengkapnya, lihat Mengelola akses ke aplikasi.

> **Note**
>
> Anda tidak dapat melihat atau menghapus pengguna dan grup dari halaman edit Portal Browser WorkSpaces Aman. Anda harus melakukan ini dari halaman edit konsol Pusat Identitas IAM Anda.

Mengubah tipe penyedia identitas

Ikuti langkah-langkah berikut untuk mengubah jenis otentikasi portal Anda kapan saja:

- Untuk mengubah dari IAM Identity Center ke Standard, ikuti langkah-langkah dithe section called “Konfigurasikan jenis otentikasi standar”.
- Untuk mengubah dari Standard ke IAM Identity Center, ikuti langkah-langkah dithe section called “Konfigurasikan jenis autentikasi Pusat Identitas IAM”.

Perubahan pada jenis penyedia identitas dapat memakan waktu hingga 15 menit untuk diterapkan, dan tidak akan secara otomatis mengakhiri sesi yang sedang berlangsung.

Anda dapat melihat perubahan jenis penyedia identitas ke portal Anda AWS CloudTrail dengan memeriksa `UpdatePortal` peristiwa. Jenis ini terlihat dalam muatan permintaan dan respons acara.

Tinjau dan luncurkan

1. Pada Langkah 5: Tinjau dan luncurkan halaman, tinjau pengaturan yang Anda pilih untuk portal web Anda. Anda dapat memilih Edit untuk mengubah pengaturan dalam bagian tertentu. Anda juga dapat mengubah pengaturan ini nanti dari tab portal Web konsol.
2. Setelah selesai, pilih Luncurkan portal web.
3. Untuk melihat status portal web Anda, pilih portal Web, pilih portal Anda, lalu pilih Lihat detail.

   Portal web memiliki salah satu status berikut:

   - Tidak lengkap - Konfigurasi portal web tidak memiliki pengaturan penyedia identitas yang diperlukan.
   - Tertunda - Portal web menerapkan perubahan pada pengaturannya.
   - Aktif - Portal web siap dan tersedia untuk digunakan.
4. Tunggu hingga 15 menit hingga portal Anda menjadi Aktif.

Langkah 2: Uji portal web Anda

Setelah membuat portal web, Anda dapat masuk ke titik akhir Browser WorkSpaces Aman untuk menelusuri situs web yang terhubung seperti yang dilakukan pengguna akhir.

Jika Anda sudah menyelesaikan langkah-langkah inithe section called “Konfigurasikan penyedia identitas”, Anda dapat melewati bagian ini dan pergi keLangkah 3: Mendistribusikan portal web Anda.

1. Buka konsol Browser WorkSpaces Aman di https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Lihat detail
3. Di bawah titik akhir portal Web, buka URL yang ditentukan untuk portal Anda. Titik akhir portal web adalah titik akses pengguna Anda akan meluncurkan portal web Anda setelah masuk dengan penyedia identitas yang dikonfigurasi untuk portal. Ini tersedia untuk umum di internet dan dapat disematkan ke jaringan Anda.
4. Pada halaman login Browser WorkSpaces Aman, pilih Masuk, SAMP, dan masukkan kredensyal SAMP Anda.
5. Saat Anda melihat halaman Sesi Anda sedang disiapkan, sesi Browser WorkSpaces Aman Anda diluncurkan. Jangan menutup atau keluar dari halaman ini.

6. Browser web diluncurkan, menampilkan URL startup Anda dan perilaku tambahan lainnya yang dikonfigurasi melalui pengaturan kebijakan browser Anda.
7. Anda sekarang dapat menelusuri situs web yang terhubung dengan memilih tautan atau memasukkan URL ke bilah alamat.

Langkah 3: Mendistribusikan portal web Anda

Ketika Anda siap untuk pengguna Anda untuk mulai menggunakan Browser WorkSpaces Aman, Anda memilih dari opsi berikut untuk mendistribusikan portal:

- Tambahkan portal Anda ke gateway aplikasi SAMP Anda untuk memungkinkan pengguna meluncurkan sesi dari IDP mereka secara langsung. Anda dapat melakukan ini melalui alur masuk yang diprakarsai IDP dengan IDP yang sesuai dengan SAMP 2.0 Anda. Untuk informasi selengkapnya, lihat pernyataan SAMP yang diprakarsai SP dan yang diprakarsai IDP di. the section called “Konfigurasikan jenis otentikasi standar” Atau, Anda dapat membuat aplikasi SAMP kustom yang dapat memberikan pengalaman otentikasi yang diprakarsai IDP dengan menggunakan alur yang diprakarsai SP. Untuk informasi selengkapnya, lihat Membuat integrasi Aplikasi Bookmark.
- Tambahkan URL portal ke situs web yang Anda miliki, dan gunakan pengalihan browser untuk mengarahkan pengguna ke portal web.
- Email URL portal ke pengguna Anda, atau tekan ke perangkat yang Anda kelola sebagai halaman beranda browser atau bookmark.

Langkah selanjutnya

Setelah membuat portal web pertama, Anda dapat melihat detail, mengedit detail, atau menghapus portal web kapan saja. Untuk informasi selengkapnya, lihat Mengelola portal web Anda.

Anda Akun AWS dapat membuat portal web di masing-masing Wilayah AWS tempat Browser WorkSpaces Aman tersedia. Setiap portal web dapat mendukung hingga 25 koneksi pengguna setiap saat. Untuk menambah jumlah portal yang dapat Anda buat di Wilayah, atau untuk mendukung lebih banyak sesi bersamaan untuk portal, lihat. the section called “Kelola kuota layanan untuk portal Anda”

Mengelola portal web Anda

Setelah Anda mengatur portal web Anda, Anda dapat melihat atau mengedit detailnya, serta menghapus portal jika tidak lagi diperlukan.

Topik

- Lihat detail portal web
- Mengedit portal web
- Hapus portal web
- Kelola kuota layanan untuk portal Anda
- Kontrol interval untuk mengautentikasi ulang token IDP SAMP
- Siapkan pencatatan akses pengguna
- Menyetel atau mengedit kebijakan browser
- Konfigurasikan Input Method Editor (IME)
- Konfigurasikan lokalisasi dalam sesi
- Mengatur kontrol akses IP (opsional)
- Aktifkan ekstensi untuk sistem masuk tunggal (opsional)
- Mengatur pemfilteran URL
- Izinkan tautan dalam (opsional)

Lihat detail portal web

Untuk melihat detail portal web

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Lihat detail.

Mengedit portal web

Untuk mengedit portal web

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Edit.

> **Note**
>
> Perubahan pada pengaturan jaringan atau pengaturan batas waktu segera mengakhiri sesi portal aktif apa pun. Pengguna terputus dan harus terhubung kembali untuk memulai sesi baru. Perubahan pada izin Clipboard, Izin transfer file, atau Cetak ke perangkat lokal berlaku dimulai dengan sesi baru pertama. Saat ini sesi aktif tidak terputus. Pengguna yang terhubung ke sesi aktif tidak terpengaruh oleh perubahan hingga mereka memutuskan sambungan dan terhubung ke sesi baru.

Hapus portal web

Untuk menghapus portal web

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Hapus.

Kelola kuota layanan untuk portal Anda

Saat Anda membuat Akun AWS, kami secara otomatis menetapkan kuota layanan default (juga disebut sebagai batas) untuk penggunaan sumber daya dengan Layanan AWS. Administrator harus mengetahui dua kuota yang mungkin perlu ditingkatkan untuk mendukung kasus penggunaannya. Kedua kuota ini adalah jumlah portal web yang dapat Anda buat di setiap wilayah, dan jumlah sesi bersamaan maksimum yang dapat Anda dukung dengan setiap jenis instans yang tersedia di setiap wilayah. Anda dapat meminta peningkatan untuk ini dari halaman Service Quotas di Konsol. AWS

Tabel berikut mencantumkan batas kuota layanan default.

Kuota default dalam akun Wilayah AWS menurut	Nilai
Portal web	3

Kuota default dalam akun Wilayah AWS menurut	Nilai
Sesi bersamaan maksimum - standard.regular	25
Sesi bersamaan maksimum - standard.large	10
Sesi bersamaan maksimum - standard.xlarge	5

> **Important**
>
> Kuota layanan mempengaruhi satu Wilayah AWS per satu. Anda harus meminta peningkatan kuota layanan di setiap Wilayah AWS tempat Anda membutuhkan lebih banyak sumber daya. Untuk informasi selengkapnya, titik akhir dan kuota Amazon WorkSpaces Secure Browser.

Meminta peningkatan kuota layanan

1. Buka dasbor AWS Support.
2. Pilih Peningkatan Batas Layanan.

   > **Important**
   >
   > WorkSpaces Kuota layanan Browser Aman memengaruhi satu Wilayah pada satu waktu. Anda harus meminta peningkatan kuota layanan di setiap Wilayah AWS di mana Anda membutuhkan lebih banyak sumber daya. Untuk informasi selengkapnya, lihat titik akhir layanan AWS.

3. Di bawah Use case description, masukkan informasi berikut:

   - Jika Anda meminta peningkatan jumlah portal web, tentukan jenis sumber daya ini, dan sertakan ID Akun AWS Anda, wilayah tempat Anda ingin kenaikan, dan nilai batas baru.
   - Jika Anda meminta peningkatan untuk sesi bersamaan maksimum, tentukan jenis sumber daya ini, dan sertakan ID Akun AWS Anda, wilayah tempat Anda ingin kenaikan, ARN portal web, dan nilai batas baru.

4. (Opsional) Untuk meminta peningkatan kuota beberapa layanan secara bersamaan, lengkapi satu permintaan peningkatan kuota di bagian Permintaan, lalu pilih Tambahkan permintaan lain.

Minta peningkatan portal

Portal adalah sumber daya dasar layanan. Setiap portal adalah asosiasi antara penyedia identitas SAMP 2.0 Anda dan koneksi jaringan Anda ke internet dan konten web pribadi apa pun. Setiap portal dapat memiliki kebijakan browser portal dan pengaturan pengguna yang terpisah, sehingga administrator biasanya akan membuat beberapa portal di wilayah yang sama untuk mengatasi kasus penggunaan yang berbeda. Misalnya, Anda dapat memberikan Grup A akses ke situs web tertentu dengan kebijakan terbatas (misalnya, Clipboard dan transfer File dinonaktifkan), dan Grup B dengan akses ke internet umum tanpa pemfilteran URL. Anda dapat membuat portal di mana pun yang didukung Wilayah AWS. Untuk melihat ketersediaan layanan saat ini, lihat AWS Services by Region.

Meminta peningkatan kuota layanan

1. Buka halaman Service Quotas di wilayah yang Anda inginkan.
2. Pilih Jumlah Portal Web.
3. Pilih Minta kenaikan di tingkat akun.
4. Di bawah Tingkatkan nilai kuota, masukkan jumlah total kuota yang Anda inginkan.

Minta peningkatan sesi bersamaan maksimum

Kuota sesi konkuren maksimum adalah jumlah pengguna tertinggi yang dapat dihubungkan secara bersamaan ke portal. Jika batas kuota layanan untuk sesi bersamaan maksimum tidak ditetapkan dengan tepat, pengguna mungkin menemukan bahwa sesi tidak tersedia saat mereka masuk. Selain meningkatkan kuota layanan ini, pelanggan juga harus memastikan bahwa VPC dan subnet mereka memiliki ruang IP yang cukup untuk mendukung sesi konkuren maksimum.

Untuk meminta peningkatan sesi bersamaan maksimum

1. Buka halaman Service Quotas di wilayah yang Anda inginkan.
2. Pilih Jumlah Sesi Serentak Maksimum per Portal untuk jenis instans yang ingin Anda tingkatkan.
3. Pilih Minta kenaikan di tingkat akun.
4. Di bawah Tingkatkan nilai kuota, masukkan jumlah total kuota yang Anda inginkan.

> **Note**
>
> Untuk kenaikan besar atau mendesak, buka halaman riwayat Service Quotas Anda, pilih tautan di kolom status permintaan Anda, tautkan ke kasus dukungan Anda, dan

tambahkan balasan dengan detail tentang kasus penggunaan Anda dan/atau urgensi. Informasi ini membantu tim layanan memprioritaskan permintaan dan memastikan kapasitas yang cukup dialokasikan untuk akun Anda.

Batasi contoh

Misalnya, asumsikan administrator mengkonfigurasi dua portal web di US East (Virginia N.) untuk 125 total pengguna. Sebelum membuat portal web, administrator mengidentifikasi portal web pertama (Portal A) akan mendukung 100 pengguna. Saat menguji alur kerja untuk pengguna ini, administrator menentukan bahwa mereka memerlukan jenis instans XL untuk mendukung streaming audio dan video selama sesi berlangsung. Portal web kedua (Portal B) harus tersedia hingga 25 pengguna untuk mendukung akses ke satu halaman web statis yang dihosting di VPC pelanggan. Saat menguji kasus penggunaan ini, administrator menentukan bahwa tipe instans standar dapat mendukung kasus penggunaan ini.

Untuk portal A, administrator harus mengirimkan permintaan peningkatan kuota layanan untuk menaikkan batas instans XL dari default wilayah (yaitu, 5) menjadi 100. Setelah terpenuhi, administrator dapat mengalokasikan kapasitas dengan mengedit portal web. Untuk portal B, administrator dapat bergerak maju tanpa meminta peningkatan kuota (yaitu, karena wilayah memiliki kuota default 25 untuk tipe instans standar).

Kelola kuota layanan

Untuk melihat kuota layanan yang dialokasikan ke akun Anda untuk setiap wilayah kapan saja, lihat halaman Service Quotas.

Kuota layanan lainnya

Anda dapat melihat dan meminta kenaikan kuota lain yang tercantum di halaman Service Quotas. Dalam praktiknya, sebagian besar pelanggan akan merasa tidak perlu meminta kenaikan untuk batasan ini. Kuota ini secara luas dikelompokkan menjadi dua jenis: Number dan Rate.

Untuk kuota Nomor, ketika Anda mengirimkan peningkatan kuota layanan untuk Jumlah portal web, Anda akan secara otomatis menerima peningkatan jumlah sub-sumber daya yang diperlukan untuk membuat portal unik. Ini akan tercermin pada halaman Service Quotas. Misalnya, jika Anda meminta peningkatan portal dari 3 menjadi 5, Anda akan secara otomatis menerima peningkatan kuota layanan dari 3 menjadi 5 untuk pengaturan browser dan pengguna. Anda memiliki opsi untuk menggunakan kembali atau membuat sub-sumber daya baru sesuai keinginan.

Pada kesempatan langka, pelanggan mungkin menemukan kasus penggunaan untuk meningkatkan jumlah atau tingkat kuota sumber daya lainnya. Misalnya, administrator mungkin ingin meningkatkan jumlah pengaturan browser untuk menguji konfigurasi portal tambahan. Permintaan kuota layanan ini akan ditinjau dan dipenuhi secara case-by-case dasar.

Untuk kuota Harga, batas tarif yang terekspos dalam Service Quotas tidak perlu disesuaikan, terlepas dari batas portal akun.

Kontrol interval untuk mengautentikasi ulang token IDP SAMP

Saat pengguna mengunjungi portal Browser WorkSpaces Aman, mereka dapat masuk untuk meluncurkan sesi streaming. Setiap sesi dimulai di halaman awal, kecuali jika mereka masuk kurang dari 5 menit yang lalu. Portal memeriksa token penyedia identitas (iDP) untuk menentukan apakah akan meminta kredensi pengguna saat meluncurkan sesi. Pengguna tanpa token iDP yang valid harus memasukkan nama pengguna, kata sandi, dan (otentikasi multifaktor opsional (MFA) untuk meluncurkan sesi streaming. Jika pengguna telah membuat token IDP SAMP dengan masuk ke iDP mereka atau aplikasi yang dilindungi oleh iDP yang sama, mereka tidak akan diminta untuk kredensyal masuk.

Jika pengguna memiliki token IDP SAMP yang valid, mereka dapat WorkSpaces mengakses Browser Aman. Anda dapat mengontrol interval yang diperlukan untuk mengautentikasi ulang token IDP SAMP.

Untuk mengontrol interval untuk mengautentikasi ulang token IDP SAMP

1. Tetapkan durasi batas waktu iDP dengan penyedia IDP SAMP Anda. Kami menyarankan untuk mengonfigurasi durasi waktu tunggu IDP Anda dengan jumlah waktu terpendek yang diperlukan pengguna untuk menyelesaikan tugasnya.

   - Untuk informasi selengkapnya tentang Okta, lihat Menegakkan masa pakai sesi terbatas untuk semua kebijakan.
   - Untuk informasi selengkapnya tentang Azure AD, lihat Mengonfigurasi kontrol sesi autentikasi.
   - Untuk informasi selengkapnya tentang Ping, lihat Sesi.
   - Untuk informasi selengkapnya AWS IAM Identity Center, lihat Mengatur durasi sesi.
2. Tetapkan ketidakaktifan portal WorkSpaces Secure Browser dan nilai batas waktu idle Anda. Nilai-nilai ini mengontrol jumlah waktu antara interaksi terakhir pengguna dan ketika sesi Browser WorkSpaces Aman berakhir karena tidak aktif. Ketika sesi berakhir, pengguna akan kehilangan

status sesi mereka (termasuk tab terbuka, konten web yang belum disimpan, dan riwayat), dan kembali ke keadaan baru pada awal sesi berikutnya. Untuk informasi selengkapnya, lihat langkah 5 di the section called “Langkah 1: Buat portal web”.

> **Note**
>
> Jika waktu sesi pengguna habis tetapi pengguna masih memiliki token SAMP iDP yang valid, mereka tidak perlu memasukkan nama pengguna dan kata sandi mereka untuk memulai sesi Browser Aman yang WorkSpaces baru. Untuk mengontrol bagaimana token diautentikasi ulang, ikuti panduan di langkah sebelumnya.

Siapkan pencatatan akses pengguna

Anda dapat mengatur pencatatan akses pengguna untuk merekam peristiwa pengguna berikut:

- Sesi mulai - Menandai awal sesi Browser WorkSpaces Aman.
- Akhir sesi - Menandai akhir sesi Browser WorkSpaces Aman.
- Navigasi URL - Log URL yang dimuat pengguna.

> **Note**
>
> Log navigasi URL direkam dari riwayat browser. URL yang tidak direkam dalam riwayat browser (baik dikunjungi dalam mode penyamaran, atau dihapus dari riwayat browser) tidak direkam dalam log. Terserah pelanggan untuk menentukan apakah akan mematikan mode penyamaran atau penghapusan riwayat dengan kebijakan browser mereka.

Selain itu, informasi berikut disertakan untuk setiap acara:

- Waktu acara
- nama pengguna
- Portal web ARN

Pelanggan bertanggung jawab untuk memahami potensi masalah hukum yang timbul dengan penggunaan Browser WorkSpaces Aman mereka, dan memastikan bahwa penggunaan Browser WorkSpaces Aman mematuhi semua hukum dan peraturan yang berlaku. Ini termasuk undang-

undang yang mengatur kemampuan pemberi kerja untuk memantau penggunaan Browser WorkSpaces Aman oleh karyawan, termasuk aktivitas yang dilakukan dalam aplikasi.

Mengaktifkan log akses pengguna di portal Browser WorkSpaces Aman Anda dapat mengakibatkan biaya dari Amazon Kinesis Data Streams. Untuk detail selengkapnya tentang harga, lihat harga Amazon Kinesis Data Streams.

Untuk mengaktifkan login akses pengguna di konsol Browser WorkSpaces Aman, di bawah Pencatatan akses pengguna, pilih ID Kinesis Stream yang ingin Anda gunakan untuk menerima data. Data yang direkam akan dikirimkan langsung ke stream tersebut.

Untuk informasi selengkapnya tentang cara membuat Aliran Data Amazon Kinesis, lihat Apa itu Amazon Kinesis Data Streams?

> **Note**
>
> Untuk menerima log dari Browser WorkSpaces Aman, Anda harus memiliki Aliran Data Kinesis Amazon yang dimulai dengan "amazon-workspaces-web-*”. Aliran data Amazon Kinesis Anda harus menonaktifkan enkripsi sisi server, atau harus digunakan untuk enkripsi sisi server. Kunci yang dikelola AWS
> Untuk informasi selengkapnya tentang menyetel enkripsi sisi server di Amazon Kinesis, lihat Bagaimana Saya Memulai Enkripsi Sisi Server? .

Log sampel

Di bawah ini adalah contoh dari setiap acara yang tersedia, termasuk Validasi, StartSession, VisitPage, dan EndSession.

Bidang berikut selalu disertakan untuk setiap acara:

- stempel waktu disertakan sebagai waktu epoch dalam milidetik.
- EventType disertakan sebagai string.
- detail disertakan sebagai objek json lain.
- PortaLarn dan UserName disertakan untuk setiap acara kecuali untuk Validasi.

```
{
  "timestamp": "1665430373875",
```

```
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

Menyetel atau mengedit kebijakan browser

Dengan Browser WorkSpaces Aman, Anda dapat mengatur kebijakan browser khusus menggunakan kebijakan Chrome yang tersedia untuk versi stabil terbaru. Ada lebih dari 300 kebijakan yang dapat Anda terapkan ke portal web. Untuk informasi selengkapnya, lihat the section called “Menetapkan kebijakan browser kustom (contoh)” dan daftar kebijakan Chrome Enterprise.

Dengan menggunakan tampilan konsol untuk membuat portal web, Anda dapat menerapkan kebijakan berikut:

- `StartURL`
- Bookmark dan folder bookmark
- Mengaktifkan dan menonaktifkan penjelajahan pribadi
- Penghapusan sejarah
- Pemfilteran URL dengan `AllowURL` dan `BlockURL`

Untuk informasi selengkapnya tentang menggunakan kebijakan tampilan konsol, lihatMemulai dengan Browser WorkSpaces Aman.

WorkSpaces Browser Aman menerapkan konfigurasi kebijakan browser dasar ke semua portal beserta kebijakan apa pun yang Anda tentukan. Anda dapat mengedit beberapa kebijakan ini dengan file JSON kustom Anda. Untuk informasi selengkapnya, lihat the section called “Edit kebijakan browser dasar”.

Topik

- Menetapkan kebijakan browser kustom (contoh)
- Edit kebijakan browser dasar

Menetapkan kebijakan browser kustom (contoh)

Anda dapat menyetel kebijakan Chrome apa pun yang didukung untuk Linux dengan mengunggah file JSON. Untuk mempelajari lebih lanjut tentang kebijakan Chrome, lihat daftar kebijakan Chrome Enterprise dan pilih platform Linux. Kemudian, cari dan tinjau kebijakan untuk versi stabil terbaru.

Dalam contoh berikut, Anda membuat portal web dengan kontrol kebijakan berikut:

- Siapkan bookmark
- Siapkan halaman startup default
- Mencegah pengguna menginstal ekstensi lain
- Mencegah pengguna menghapus riwayat
- Mencegah pengguna mengakses mode penyamaran
- Pra-instal ekstensi plug-in Okta untuk semua sesi.

Topik

- Langkah 1: Buat portal web
- Langkah 2: Kumpulkan kebijakan
- Langkah 3: Buat file kebijakan JSON kustom
- Langkah 4: Tambahkan kebijakan Anda ke template
- Langkah 5: Unggah file JSON kebijakan Anda ke portal web Anda

Langkah 1: Buat portal web

Untuk mengunggah file JSON kebijakan Chrome Anda, Anda harus membuat portal Browser WorkSpaces Aman. Untuk informasi selengkapnya, lihat the section called “Langkah 1: Buat portal web”.

Langkah 2: Kumpulkan kebijakan

Cari dan temukan kebijakan yang Anda inginkan dari Kebijakan Chrome. Anda kemudian menggunakan kebijakan untuk membuat file JSON di langkah berikutnya.

1. Buka daftar kebijakan Chrome Enterprise.
2. Pilih platform Linux, lalu pilih versi Chrome terbaru.
3. Cari kebijakan yang ingin Anda tetapkan. Untuk contoh ini, cari ekstensi untuk menemukan kebijakan untuk mengelolanya. Setiap kebijakan mencakup deskripsi, nama preferensi Linux, dan nilai sampel.
4. Dari hasil pencarian, ada 3 kebijakan yang memenuhi persyaratan bisnis jika digunakan bersama:
   - ExtensionSettings— Menginstal ekstensi di awal browser.
   - ExtensionInstallBlocklist— Mencegah ekstensi tertentu agar tidak diinstal.
   - ExtensionInstallAllowlist— Memungkinkan ekstensi tertentu dipasang.
5. Kebijakan tambahan memenuhi persyaratan yang tersisa;
   - ManagedBookmarks— Menambahkan bookmark ke halaman web.
   - RestoreOnStartupURL — Mengkonfigurasi halaman web mana yang dibuka setiap kali jendela browser baru diluncurkan.
   - AllowDeletingBrowserHistory— Mengkonfigurasi apakah pengguna dapat menghapus riwayat penjelajahan mereka.

- IncognitoModeAvailability— Mengkonfigurasi apakah pengguna dapat mengakses mode penyamaran.

Langkah 3: Buat file kebijakan JSON kustom

Buat file JSON menggunakan editor teks, templat, dan kebijakan yang Anda temukan di langkah sebelumnya.

1. Buka editor teks.
2. Salin dan tempel template berikut ke editor teks Anda:

```
{
  "chromePolicies":
    {
        "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Bookmark 1",
                    "url": "bookmark-url-1"
                },
                {
                    "name": "Bookmark 2",
                    "url": "bookmark-url-2"
                },
            ]
        },
        "RestoreOnStartup":
        {
            "value": 4
        },
        "RestoreOnStartupURLs":
        {
            "value":
            [
                "startup-url"
            ]
        },
        "ExtensionInstallBlocklist": {
            "value": [
```

```
                "insert-extensions-value-to-block",
            ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
                "insert-extensions-value-to-allow",
            ]
        },
        "ExtensionSettings":
        {
            "value":
            {
                "insert-extension-value-to-force-install":
                {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                },
            }
        },
        "AllowDeletingBrowserHistory":
        {
            "value": should-allow-history-deletion
        },
        "IncognitoModeAvailability":
        {
            "value": incognito-mode-availability
        }
    }
}
```

Langkah 4: Tambahkan kebijakan Anda ke template

Tambahkan kebijakan kustom Anda ke template untuk setiap kebutuhan bisnis.

1. Siapkan URL bookmark.
   a. Di bawah `value` tombol, tambahkan pasangan `name` dan `url` kunci untuk setiap bookmark yang ingin Anda tambahkan.
   b. Atur `bookmark-url-1` ke `https://www.amazon.com`.

c. Atur `bookmark-url-2` ke `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`.

```
    "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Amazon",
                    "url": "https//www.amazon.com"
                },
                {
                    "name": "Bookmark 2",
                    "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
                },
            ]
        },
```

2. Siapkan URL startup. Kebijakan ini memungkinkan administrator untuk menyetel halaman web yang ditampilkan saat pengguna meluncurkan jendela browser baru.

   a. Atur `RestoreOnStartup` ke `4` . Ini menetapkan `RestoreOnStartup` tindakan untuk membuka daftar URL. Anda juga dapat menggunakan tindakan lain pada URL startup Anda. Untuk informasi selengkapnya, lihat daftar kebijakan Chrome Enterprise.

   b. Setel `RestoreOnStartupURLs` ke https://www.aboutamazon.com/news.

```
     "RestoreOnStartup":
        {
            "value": 4
        },
    "RestoreOnStartupURLs":
        {
            "value":
            [
                "https://www.aboutamazon.com/news"
            ]
        },
```

3. Untuk mencegah pengguna menghapus riwayat browser mereka, atur `AllowDeletingBrowserHistory` kefalse.

```
"AllowDeletingBrowserHistory":
   {
       "value": false
   },
```

4. Untuk menonaktifkan akses ke akses mode Penyamaran bagi pengguna Anda, setel `IncognitoModeAvailability` ke. 1

```
"IncognitoModeAvailability":
   {
       "value": 1
   }
```

5. Tetapkan dan terapkan plug-in Okta dengan kebijakan berikut:

   - `ExtensionSettings`— Menginstal ekstensi di awal browser. Nilai ekstensi tersedia dari halaman bantuan plug-in Okta.
   - `ExtensionInstallBlocklist`— Mencegah ekstensi tertentu agar tidak diinstal. Gunakan * nilai untuk mencegah semua ekstensi secara default. Administrator dapat mengontrol ekstensi mana yang akan diizinkan pada file. `ExtensionInstallAllowlist`
   - `ExtensionInstallAllowlist`memungkinkan Anda untuk menginstal ekstensi tertentu. Karena `ExtensionInstallBlocklist` diatur ke*, tambahkan nilai plug-in Okta di sini untuk mengizinkannya.

   Berikut ini menunjukkan contoh kebijakan untuk mengaktifkan plug-in Okta:

```
"ExtensionInstallBlocklist": {
    "value": [
        "*",
        ]
},
"ExtensionInstallAllowlist": {
    "value": [
```

```
                "glnpjglilkicbckjpbgcfkogebgllemb",
            ]
        },
        "ExtensionSettings": {
            "value": {
                "glnpjglilkicbckjpbgcfkogebgllemb": {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
            }
        }
```

Langkah 5: Unggah file JSON kebijakan Anda ke portal web Anda

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, lalu pilih Portal Web.
3. Pilih portal web Anda, lalu pilih Edit.
4. Pilih Pengaturan kebijakan, lalu pilih Unggah file JSON.
5. Pilih Pilih File. Arahkan ke, pilih, dan unggah file JSON Anda.
6. Pilih Simpan.

Edit kebijakan browser dasar

Untuk memberikan layanan, WorkSpaces Secure Browser menerapkan kebijakan browser dasar ke semua portal. Kebijakan dasar ini diterapkan selain kebijakan yang Anda tentukan dari tampilan konsol atau upload JSON. Berikut ini adalah daftar kebijakan yang diterapkan oleh layanan dalam format JSON:

```
{
    "chromePolicies":
    {
        "DefaultDownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadDirectory": {
```

```
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadRestrictions": {
            "value": 1
        },
        "URLBlocklist": {
            "value": [
                "file://",
                "http://169.254.169.254",
                "http://[fd00:ec2::254]",
            ]
        },
        "URLAllowlist": {
            "value": [
                "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
                "file:///opt/appstream/tmp/TemporaryFiles",
            ]
        }
    }
}
```

Pelanggan tidak dapat melakukan perubahan pada kebijakan berikut:

- `DefaultDownloadDirectory`Kebijakan ini tidak dapat diedit. Layanan menimpa setiap perubahan pada kebijakan ini.
- `DownloadDirectory`Kebijakan ini tidak dapat diedit. Layanan menimpa setiap perubahan pada kebijakan ini.

Pelanggan dapat memperbarui kebijakan berikut untuk portal web mereka:

- `DownloadRestrictions`— Default diatur 1 untuk mencegah unduhan yang diidentifikasi sebagai berbahaya oleh Penjelajahan Aman Chrome. Untuk informasi selengkapnya, lihat Mencegah pengguna mengunduh file berbahaya. Anda dapat mengatur nilai dari `0` ke`4`.
- `URLBlocklist`Kebijakan `URLAllowlist` dan dapat diperluas dengan menggunakan fitur Pemfilteran URL tampilan konsol atau unggahan JSON. Namun, URL dasar tidak dapat ditimpa. Kebijakan ini tidak terlihat dari file JSON yang diunduh dari portal web Anda. Namun, jika Anda mengunjungi “chrome: //policy” selama sesi, browser jarak jauh akan menampilkan kebijakan yang diterapkan.

Konfigurasikan Input Method Editor (IME)

Input Method Editor (IME) adalah utilitas yang menyediakan opsi kepada pengguna akhir untuk memasukkan teks dalam bahasa yang menggunakan tata letak keyboard selain keyboard QWERTY. IME membantu pengguna memasukkan teks dalam bahasa dengan set bahasa yang lebih besar dan lebih kompleks, seperti Jepang, China, dan Korea. WorkSpaces Sesi Browser Aman menyertakan dukungan IME secara default. Pengguna dapat memilih bahasa alternatif dari toolbar IME dalam sesi atau dengan menggunakan pintasan keyboard.

Bahasa berikut saat ini didukung oleh IME Browser WorkSpaces Aman:

- Bahasa Inggris
- Bahasa Mandarin Sederhana (Pinyin)
- Tionghoa Tradisional (Bopomofo)
- Bahasa Jepang
- Bahasa Korea

Untuk memilih bahasa dari toolbar IME, lakukan hal berikut:

1. Pilih drop-down pemilih bahasa yang terletak di sisi kanan bilah panel atas hitam. Secara default, pemilih akan menampilkan en, untuk bahasa Inggris.
2. Di menu tarik-turun, pilih bahasa yang diinginkan.
3. Di submenu yang muncul setelah memilih bahasa, pilih detail bahasa tambahan.

Untuk memilih bahasa menggunakan pintasan keyboard, gunakan yang berikut ini:

- Semua IME
  - Untuk memajukan IME (atau pindah ke tata letak keyboard kanan), tekanShift+Control+Left Alt.
- Bahasa Jepang
  - Untuk memilih Hiragana, tekan. F6
  - Untuk memilih Katakana, tekan. F7
  - Untuk memilih bahasa Latin, tekanF10.
  - Untuk memilih Wide Latin, tekanF9.
  - Untuk memilih Input Langsung, tekan ALT +, ALT+@, Zenkaku Hankaku.

- Bahasa Korea
  - Untuk memilih Hangul, tekanShift+Space.
  - Untuk memilih Hanja, tekanF9.

Untuk menghapus bilah alat dan menu IME, atau untuk mematikan keyboard di layar dari sesi Browser WorkSpaces Aman Anda, hubungi. AWS Support

Konfigurasikan lokalisasi dalam sesi

Ketika pengguna memulai sesi, WorkSpaces Secure Browser mendeteksi bahasa browser lokal pengguna dan pengaturan zona waktu dan menerapkannya ke sesi. Ini memengaruhi bahasa tampilan selama sesi, dan membantu memastikan bahwa waktu yang ditampilkan cocok dengan waktu saat ini di lokasi pengguna.

Daftar berikut menunjukkan kode bahasa yang saat ini didukung oleh WorkSpaces Secure Browser. Jika browser lokal pengguna diatur untuk menggunakan kode bahasa yang tidak didukung, sesi default ke bahasa Inggris (en-US).

- Bahasa Jerman
  - de — Jerman
  - De-at — Jerman (Austria)
  - De-de — Jerman (Jerman)
  - De-ch — Jerman (Swiss)
  - De-li — Jerman (Liechtenstein)
- Bahasa Inggris
  - en — Bahasa Inggris
  - En-au — Inggris (Australia)
  - En-CA — Inggris (Kanada)
  - En-in — Inggris (Indonesia)
  - en-NZ — Inggris (Selandia Baru)
  - En-za — Inggris (Afrika Selatan)
  - en-GB — Inggris (Inggris Raya)
  - en-US — Inggris (Amerika Serikat)
- Bahasa Spanyol

  - es — Spanyol
  - Es-ar — Spanyol (Argentina)
  - Es-CL - Spanyol (Chili)
  - Es-co — Spanyol (Kolombia)
  - es-CR - Spanyol (Kosta Rika)
  - Es-hn — Spanyol (Honduras)
  - es-419 — Spanyol (Amerika Latin)
  - es-MX — Spanyol (Meksiko)
  - es-PE - Spanyol (Peru)
  - ES-es — Spanyol (Spanyol)
  - es-US - Spanyol (Amerika Serikat)
  - es-UY - Spanyol (Uruguay)
  - Es-ve — Spanyol (Venezuela)
- Prancis
  - fr — Prancis
  - fr-Ca — Prancis (Kanada)
  - FR-fr - Prancis (Prancis)
  - FR-ch — Prancis (Swiss)
- orang Indonesia
  - id — Indonesia
  - ID-ID — Bahasa Indonesia (Indonesia)
- Bahasa Italia
  - itu — Italia
  - IT-it - Italia (Italia)
  - IT-ch — Italia (Swiss)
- Bahasa Jepang
  - ja — Jepang
  - Ja-jp - Jepang (Jepang)
- Bahasa Korea
  - ko — Korea

  - Ko-kr — Korea (Korea)
- Bahasa Portugis
  - pt — Portugis
  - Pt-BR - Portugis (Brasil)
  - Pt-PT — Portugis (Portugal)
- Mandarin
  - zh — Bahasa Mandarin
  - Zh-CN - Mandarin (Tiongkok)
  - Zh-HK - China (Hong Kong)
  - Zh-TW - Bahasa Mandarin (Taiwan)

Bahasa sesi ditentukan dalam urutan prioritas berikut:

1. ForcedLanguagesKebijakan dalam pengaturan browser portal web. Untuk informasi lebih lanjut, lihat ForcedLanguages.
2. Pengaturan bahasa browser lokal pengguna akhir.
3. Nilai default, Bahasa Inggris (en-US).

Zona waktu ditentukan oleh pengaturan zona waktu lokal yang ditentukan di browser pengguna akhir. Jika pengaturan zona waktu tidak valid, UTC akan digunakan.

Komponen berikut di WorkSpaces Secure Browser mendukung lokalisasi:

- WorkSpaces Halaman masuk Browser Aman
- WorkSpaces Pesan status portal Browser Aman (termasuk memuat pesan dan kesalahan)
- Browser Chrome
- Menu Konteks Sistem dan Simpan sebagai jendela

Untuk mengatur pengaturan browser lokal pengguna, lakukan salah satu hal berikut:

- Di Chrome, pilih Pengaturan, pilih Bahasa, lalu urutkan bahasa berdasarkan preferensi.
- Di Firefox, pilih Pengaturan, Umum, Bahasa, dan pilih bahasa dari menu tarik-turun.
- Di Edge, pilih Pengaturan, pilih Bahasa, lalu urutkan bahasa berdasarkan preferensi.

Mengatur kontrol akses IP (opsional)

WorkSpaces Secure Browser memungkinkan Anda mengontrol alamat IP mana portal web Anda dapat diakses. Dengan menggunakan pengaturan akses IP, Anda dapat menentukan dan mengelola grup alamat IP tepercaya, dan hanya mengizinkan pengguna mengakses portal mereka ketika mereka terhubung ke jaringan tepercaya.

Secara default, WorkSpaces Secure Browser memungkinkan pengguna untuk mengakses portal web mereka dari mana saja. Grup kontrol akses IP bertindak sebagai firewall virtual yang memfilter alamat IP mana yang dapat digunakan pengguna untuk terhubung ke portal web. Ketika dikaitkan dengan portal web Anda, pengaturan akses IP akan mendeteksi IP pengguna sebelum otentikasi untuk menentukan apakah mereka memenuhi syarat untuk terhubung. Setelah terhubung, WorkSpaces Secure Browser terus memantau alamat IP pengguna untuk memastikan mereka tetap terhubung dari jaringan tepercaya. Jika IP pengguna berubah, WorkSpaces Secure Browser akan mendeteksi dan mengakhiri sesi.

Untuk menentukan rentang alamat CIDR, tambahkan aturan ke grup kontrol akses IP Anda, lalu kaitkan grup dengan portal web Anda. Anda dapat mengaitkan setiap pengaturan akses IP dengan satu atau lebih portal web. Untuk menentukan alamat IP publik dan rentang alamat IP untuk jaringan terpercaya Anda, tambahkan aturan ke grup kontrol akses IP. Jika pengguna Anda mengakses portal web mereka melalui gateway NAT atau VPN, Anda harus membuat aturan yang memungkinkan lalu lintas dari alamat IP publik untuk gateway NAT atau VPN.

> **Note**
>
> Pelanggan bertanggung jawab untuk memahami potensi masalah hukum yang timbul dengan penggunaan Browser WorkSpaces Aman mereka, dan harus memastikan bahwa penggunaan Browser WorkSpaces Aman mematuhi semua hukum dan peraturan yang berlaku. Ini termasuk undang-undang yang mengatur kemampuan pemberi kerja untuk memantau penggunaan Browser WorkSpaces Aman oleh karyawan, termasuk aktivitas yang dilakukan dalam aplikasi.

Buat grup kontrol akses IP

Untuk membuat grup kontrol akses IP, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi, pilih kontrol akses IP.
3. Pilih Buat grup kontrol akses IP.
4. Dalam kotak dialog Buat grup kontrol akses IP, masukkan nama (wajib) dan deskripsi (opsional) untuk grup.
5. Masukkan alamat IP atau rentang IP CIDR yang akan dikaitkan dengan Sumber, dan Deskripsi (opsional).
6. Di bawah Tag, pilih apakah akan menandai pasangan nilai kunci untuk setiap grup kontrol akses IP.
7. Setelah selesai menambahkan aturan dan tag, pilih Simpan.

Kaitkan pengaturan akses IP dengan portal web

Untuk mengaitkan grup kontrol akses IP dengan portal web yang ada, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi, pilih Portal Web.
3. Pilih portal web, dan pilih Edit.
4. Di bawah grup kontrol akses IP, dan pilih grup kontrol akses IP untuk portal web.
5. Pilih Simpan.

Untuk mengaitkan grup kontrol akses IP saat membuat portal web baru, ikuti langkah-langkah ini.

1. Selesaikan langkah 1 hingga 4 the section called “Konfigurasikan pengaturan portal” untuk mengakses Kontrol Akses IP (opsional).
2. Pilih Buat kontrol akses IP.
3. Dalam Buat Grup IP kotak dialog, masukkan nama (wajib) dan deskripsi (opsional) untuk grup.
4. Masukkan alamat IP atau rentang IP CIDR yang akan dikaitkan dengan Sumber, dan Deskripsi (opsional).
5. Di bawah Tag, pilih apakah akan menandai pasangan nilai kunci untuk setiap grup kontrol akses IP.

6. Setelah selesai menambahkan aturan dan tag, pilih Buat kontrol akses IP.
7. Grup kontrol akses IP Anda akan dikaitkan dengan portal web ini saat diluncurkan.

Edit grup kontrol akses IP

Anda dapat menghapus aturan dari pengaturan akses IP kapan saja. Jika Anda menghapus aturan yang digunakan untuk mengizinkan koneksi ke portal web, setiap pengguna dengan sesi saat ini akan terputus dari portal web.

Untuk mengedit grup kontrol akses IP, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi, pilih kontrol akses IP.
3. Pilih grup target Anda dan pilih Edit.
4. Edit aturan yang ada Sumber dan Deskripsi (opsional), atau tambahkan aturan tambahan.
5. Di bawah Tag, pilih apakah akan menandai pasangan nilai kunci untuk setiap grup kontrol akses IP.
6. Setelah selesai menambahkan aturan dan tag, pilih Simpan.
7. Jika Anda memperbarui pengaturan akses IP yang ada, tunggu hingga 15 menit agar aturan baru atau yang telah diedit berlaku.

Menghapus grup kontrol akses IP

Anda dapat menghapus aturan dari grup kontrol akses IP kapan saja. Jika Anda menghapus aturan yang digunakan untuk mengizinkan koneksi ke portal web, setiap pengguna dengan sesi saat ini akan terputus dari portal web.

Untuk menghapus grup kontrol akses IP, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi, pilih grup kontrol akses IP.
3. Pilih grup dan pilih Hapus.

Aktifkan ekstensi untuk sistem masuk tunggal (opsional)

Anda dapat mengaktifkan ekstensi agar pengguna akhir Anda memiliki pengalaman masuk portal yang lebih baik. Misalnya, jika Anda menggunakan Okta sebagai penyedia identitas SAMP 2.0 portal Anda (IDP), dan Anda juga menggunakannya sebagai idP untuk situs web yang ingin dikunjungi pengguna selama sesi, Anda dapat meneruskan cookie masuk Okta ke sesi dengan ekstensi. Setelah itu, ketika pengguna mengunjungi situs web yang memerlukan cookie domain Okta, mereka dapat mengakses situs web tanpa harus masuk selama sesi berlangsung.

Ekstensi ini didukung di browser Chrome dan Firefox. Ekstensi ini memungkinkan sinkronisasi cookie untuk domain yang diizinkan dari pengguna yang masuk ke sesi. Ekstensi tidak mengharuskan pengguna untuk masuk, dan berfungsi di belakang layar untuk mengaktifkan sinkronisasi cookie tanpa mengharuskan pengguna untuk mengambil tindakan apa pun setelah instalasi. Tidak ada data yang disimpan oleh ekstensi.

Pengguna diminta untuk menginstal ekstensi ketika mereka masuk ke portal.

Secara default, ekstensi tidak diaktifkan di Chrome di jendela Penyamaran atau jendela Penjelajahan Pribadi Firefox. Pengguna dapat mengaktifkannya secara manual. Untuk informasi selengkapnya tentang Chrome, lihat Ekstensi dalam mode Penyamaran. Untuk informasi selengkapnya tentang Firefox, lihat Ekstensi di Penjelajahan Pribadi.

Anda dapat memperbarui konfigurasi pengaturan pengguna portal yang ada, atau saat membuat portal web untuk pertama kalinya. Pertama, tentukan domain mana yang Anda butuhkan untuk IDP dan situs web SAMP Anda. Anda dapat menambahkan hingga 10 domain.

Anda bertanggung jawab untuk menguji dan mengidentifikasi domain yang sesuai untuk cookie yang akan disinkronkan. Perubahan mungkin diperlukan di iDP atau tingkat otentikasi situs web untuk memastikan sistem masuk tunggal berfungsi seperti yang diharapkan.

Untuk melihat domain mana yang akan digunakan dengan iDP yang paling umum, lihat tabel berikut:

IDP dan domain

IdP	Domain
Okta	okta.com
ID Entra	microsoftonline.com

IdP	Domain
Pusat Identitas AWS	awsapps.com
Satu Login	onelogin.com
duet	duosecurity.com

Selanjutnya, kunjungi portal web Anda di konsol. Kemudian, izinkan ekstensi dan tambahkan cookie domain mana yang harus disinkronkan. Ikuti langkah-langkah di bawah ini untuk membuat portal baru dengan ekstensi yang diizinkan, atau untuk memperbarui portal yang ada.

Untuk mengizinkan ekstensi saat membuat portal web baru, ikuti langkah-langkah ini:

1. Ikuti langkah-langkahnya the section called “Langkah 1: Buat portal web” sampai Anda tibathe section called “Konfigurasikan pengaturan pengguna”.
2. Untuk langkah 1the section called “Konfigurasikan pengaturan pengguna”, di bawah Izin pengguna, pilih Diizinkan untuk mengaktifkan ekstensi untuk portal web Anda.
3. Masukkan domain untuk sinkronisasi cookie, dan pilih Tambahkan domain baru.
4. Selesaikan langkah-langkah di the section called “Konfigurasikan pengaturan pengguna” dan bagian yang tersisa the section called “Langkah 1: Buat portal web” untuk membuat portal web Anda.

Untuk menambahkan ekstensi ke portal web yang ada, ikuti langkah-langkah berikut:

1. Buka konsol Browser WorkSpaces Aman di https://console.aws.amazon.com/workspaces-web/home.
2. Pilih portal web yang akan diedit.
3. Pilih Pengaturan pengguna, Izin pengguna, dan Diizinkan untuk mengaktifkan ekstensi untuk portal web Anda.
4. Masukkan domain untuk sinkronisasi cookie, pilih Tambahkan domain baru.
5. Simpan perubahan portal Anda. Portal akan meminta pengguna untuk menginstal ekstensi dalam waktu 15 menit.

Untuk mengedit domain atau menghapus ekstensi, ikuti langkah-langkah berikut:

1. Buka konsol Browser WorkSpaces Aman di https://console.aws.amazon.com/workspaces-web/home.
2. Pilih portal web yang akan diedit.
3. Pilih Pengaturan pengguna, Izin pengguna, dan Tidak diizinkan untuk menghapus ekstensi untuk portal web Anda.
4. Hapus atau edit domain individual.
5. Setelah dihapus, sesi tidak akan lagi menyinkronkan cookie, bahkan jika pengguna memiliki ekstensi Browser WorkSpaces Aman yang diinstal di browser mereka.

Untuk detail tentang pengalaman pengguna dengan ekstensi, lihatthe section called “Ekstensi untuk sistem masuk tunggal”.

Mengatur pemfilteran URL

Anda dapat menggunakan Kebijakan Chrome untuk memfilter URL mana yang dapat diakses pengguna dari browser jarak jauh mereka. Kebijakan Chrome menyediakan dua mekanisme untuk memfilter URL: URLAllowList dan URLBlockList. Anda dapat menggunakan antarmuka konsol Browser WorkSpaces Aman untuk mengonfigurasi pemfilteran URL sebagai setelan portal, atau Anda dapat menambahkannya sebagai bagian dari pernyataan JSON kustom Anda (baik di editor sebaris, atau sebagai unggahan file JSON).

Untuk mengatur pemfilteran URL menggunakan konsol

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Lihat detail.
3. Untuk pemfilteran URL, pilih dari opsi berikut:

   - Izinkan akses ke semua URL: Secara default, portal web memungkinkan akses ke semua URL. Anda dapat menambahkan situs web tertentu ke daftar BlockUrl untuk mencegah pengguna mengunjungi situs tersebut selama sesi. Misalnya, menambahkan www.anycorp.com ke daftar BlockUrl akan mencegah pengguna menavigasi ke www.anycorp.com selama sesi mereka.
   - Blokir akses ke semua URL: Secara default, portal web memblokir akses ke semua URL. Anda dapat menambahkan situs web tertentu ke daftar yang diizinkan URL untuk menyusun daftar situs web yang dapat dikunjungi pengguna, dan memblokir lalu lintas ke situs web lain.

Pertimbangkan untuk menambahkan setiap URL sebagai bookmark untuk mengaktifkan akses 1-klik bagi pengguna selama sesi mereka.

- Konfigurasi lanjutan: Pilih opsi ini untuk membuat daftar allowUrl dan BlockUrl secara paralel. Daftar yang diizinkan URL memiliki prioritas di atas daftar blokir URL. Opsi ini memungkinkan pemfilteran URL berdasarkan jalur. Misalnya, Anda dapat menambahkan www.anycorp.com ke daftar blokir, dan kemudian menambahkan www.anycorp.com/hr ke daftar izinkan. Ini memungkinkan pengguna untuk mengunjungi www.anycorp.com/hr, tetapi mereka tidak akan dapat mengakses jalur URL lain, seperti www.anycorp.com/finance.

Untuk panduan selengkapnya tentang penggunaan blokir dan izinkan URL, lihat Mengizinkan atau memblokir akses ke situs web. Tambahkan URL ke daftar ini mengikuti format filter daftar blokir Chrome untuk hasil terbaik. Untuk informasi selengkapnya, lihat format filter daftar blokir URL.

Untuk mengatur pemfilteran URL menggunakan editor JSON atau unggahan file

1. Dari modul Pengaturan kebijakan, pilih Editor JSON dan lewati modul UI konsol untuk tampilan Editor atau Unggah File.

   - Editor memungkinkan pelanggan membuat pernyataan kebijakan khusus sebaris di konsol. Editor menyoroti kesalahan dalam pernyataan JSON selama pembuatan kebijakan.
   - Pengunggahan file memungkinkan pelanggan untuk menambahkan file JSON yang dibuat di luar konsol (seperti diekspor dari browser Chrome yang ada).
2. Lihat detail Kebijakan Chrome untuk URLAllowList dan URLBlocklist untuk memformat daftar allow/DenyURL dengan benar untuk portal web Anda. Untuk informasi selengkapnya, lihat UrlAllowList dan URLBlockList.

Izinkan tautan dalam (opsional)

Saat pengguna masuk ke Browser WorkSpaces Aman, mereka memulai sesi di halaman beranda yang ditetapkan oleh administrator. Anda juga dapat mengizinkan portal menerima tautan dalam yang menghubungkan pengguna ke situs web tertentu selama sesi. Saat deep link dipilih, portal menampilkan URL yang ditentukan di deep link. Tautan ditampilkan di samping halaman beranda yang dikonfigurasi untuk memulai sesi, atau dengan sendirinya jika sesi sudah berlangsung. Fitur ini memungkinkan administrator untuk membuat pengalaman pengguna yang lebih dinamis dengan Browser WorkSpaces Aman. Untuk mengizinkan izin tautan dalam, pilih Diizinkan saat membuat

pengaturan pengguna. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan pengaturan pengguna”.

Deep link membuka halaman dalam sesi Browser WorkSpaces Aman. Jika sesi sudah berjalan, itu akan membuka deep link di tab baru. Jika sesi belum berjalan, itu akan membuka URL tautan dalam di tab baru, dan halaman beranda default portal di tab terpisah. Jika deep link berisi lebih dari satu URL, itu akan menampilkan URL tautan dalam yang terdaftar pertama dalam fokus, dengan setiap URL berikutnya (termasuk halaman beranda default) dibuka di tab terpisah.

Deep link harus memenuhi persyaratan berikut:

- Portal harus memiliki izin tautan dalam yang disetel ke Diizinkan. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan pengaturan pengguna”.
- Situs yang ingin Anda tautkan dalam harus dikodekan URL. Misalnya, untuk menautkan pengguna ke “https://www.example.com/?query=true”, perbarui tautan ke http%3A%2F %2Fwww.example.com%2F%3FQuery%3DTrue.
- Tambahkan URL ke URL portal yang diizinkan dalam format berikut, di mana UUID adalah id portal:

  https://<uuid>.workspaces-web.com/? deepLinks=https%3A%2F%2Fwww.example.com%2F %3FQuery%3DTrue
- Deeplink dapat berisi hingga 10 URL, digambarkan dengan koma. Sebagai contoh:

  https://<uuid>.workspaces-web.com/? deeplinks=https%3A%2f%2fwww.example.com%2f%3f %3fquery%3dTrue, http%3A%2F%2Fwww.example.com%2f%3FQuery%3DTrue2, Http%3A %2F%2Fwww.example.com%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f %2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%ery%3dtrue3, https %3a%2f %2fwww.example.com%2f%3fquery%3dtrue4

Setiap pengguna yang Anda bagikan tautan portal ini dapat memanipulasi nilai tautan dalam untuk mengunjungi situs web, jika domain tersebut dapat dijangkau dari portal dan bukan pada daftar blokir URL. Untuk membuat daftar izin atau daftar blokir yang membatasi untuk mencegah pengguna mengunjungi domain yang tidak diinginkan dengan portal Anda, gunakan pemfilteran URL. Daftar yang diizinkan dan daftar blokir untuk portal dapat diedit dengan pemfilteran URL di pengaturan browser portal Anda. Untuk informasi selengkapnya, lihat the section called “Mengatur pemfilteran URL” dan Izinkan atau blokir akses ke situs web.

Keamanan di Amazon WorkSpaces Secure Browser

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

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

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon WorkSpaces Secure Browser, lihat AWS Services in Scope by Compliance Program .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, dan undang-undang dan peraturan yang berlaku yang berlaku untuk data Anda.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon WorkSpaces Secure Browser. Ini menunjukkan kepada Anda cara mengonfigurasi Amazon WorkSpaces Secure Browser untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Amazon WorkSpaces Secure Browser Anda.

Konten

- Perlindungan data di Amazon WorkSpaces Secure Browser
- Identity and Access Management untuk Amazon WorkSpaces Secure Browser
- Respons insiden di Amazon WorkSpaces Secure Browser
- Validasi kepatuhan untuk Amazon WorkSpaces Secure Browser
- Ketahanan di Browser Aman Amazon WorkSpaces
- Keamanan infrastruktur di Amazon WorkSpaces Secure Browser
- Analisis konfigurasi dan kerentanan di Amazon WorkSpaces Secure Browser
- Praktik terbaik keamanan untuk Amazon WorkSpaces Secure Browser

Perlindungan data di Amazon WorkSpaces Secure Browser

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon WorkSpaces Secure Browser. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat Model Tanggung Jawab AWS Bersama dan posting GDPR blog di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management ()IAM. Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Browser WorkSpaces Aman atau lainnya Layanan AWS menggunakan konsol,API, AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal,

kami sangat menyarankan agar Anda tidak menyertakan informasi kredensil dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi data

Amazon WorkSpaces Secure Browser mengumpulkan data kustomisasi portal, seperti pengaturan browser, pengaturan pengguna, pengaturan jaringan, informasi penyedia identitas, data penyimpanan kepercayaan, dan data sertifikat penyimpanan kepercayaan. WorkSpaces Secure Browser juga mengumpulkan data kebijakan browser, preferensi pengguna (untuk pengaturan browser), dan log sesi. Data yang dikumpulkan disimpan di Amazon DynamoDB dan Amazon S3. WorkSpaces Browser Aman digunakan AWS Key Management Service untuk enkripsi.

Untuk mengamankan konten Anda, ikuti panduan ini:

- Terapkan akses hak istimewa paling sedikit dan buat peran khusus yang akan digunakan untuk tindakan Browser WorkSpaces Aman. Gunakan IAM templat untuk membuat peran Akses Penuh atau peran Hanya Baca. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk Browser WorkSpaces Aman.
- Lindungi data dari ujung ke ujung dengan menyediakan kunci yang dikelola pelanggan, sehingga WorkSpaces Secure Browser dapat mengenkripsi data Anda saat istirahat dengan kunci yang Anda berikan.
- Hati-hati dengan berbagi domain portal dan kredensi pengguna:
  - Admin diminta untuk masuk ke WorkSpaces konsol Amazon, dan pengguna diharuskan masuk ke portal Browser WorkSpaces Aman.
  - Siapa pun di internet dapat mengakses portal web, tetapi mereka tidak dapat memulai sesi kecuali mereka memiliki kredensi pengguna yang valid ke portal.
- Pengguna dapat secara eksplisit mengakhiri sesi mereka dengan memilih End Session. Ini membuang instance yang menghosting sesi browser, dan menghasilkan isolasi browser.

WorkSpaces Secure Browser mengamankan konten dan metadata secara default dengan mengenkripsi semua data sensitif. AWS KMS Ini mengumpulkan kebijakan browser dan preferensi pengguna untuk menegakkan kebijakan dan pengaturan selama sesi Browser WorkSpaces Aman. Jika ada kesalahan saat menerapkan pengaturan yang ada, pengguna tidak dapat mengakses sesi baru dan tidak dapat mengakses situs internal perusahaan dan aplikasi SaaS.

Enkripsi diam

Enkripsi saat istirahat dikonfigurasi secara default. Data khusus pelanggan yang digunakan di Browser WorkSpaces Aman dienkripsi menggunakan. AWS KMS WorkSpaces Secure Browser menyediakan enkripsi saat istirahat untuk sumber daya yang Anda buat. Layanan menerima Kunci yang Dikelola AWS KMS Pelanggan pada pembuatan sumber daya, dan jika tidak disediakan, Kunci yang AWS Dimiliki akan digunakan untuk mengenkripsi sumber daya saat istirahat. Layanan mengenkripsi dokumen Kebijakan Browser yang dapat Anda berikan untuk menyesuaikan sesi browser Anda, serta konfigurasi penyedia identitas Anda, dan menampilkan nama untuk portal Anda. Informasi ini akan tetap dienkripsi menggunakan Kunci yang Dikelola Pelanggan, atau Kunci yang AWS Dimiliki, saat disimpan di backend kami.

Anda dapat memutuskan kunci mana yang akan digunakan saat Anda membuat sumber daya Browser WorkSpaces Aman. Jika data yang merupakan bagian dari sumber daya tersebut dienkripsi, Browser WorkSpaces Aman menerima `customerManagedKeyArn` bidang tersebut sebagai bagian dari file. `create` API Kunci yang disediakan harus berupa AWS KMS kunci Simetris, dan administrator yang membuat sumber daya menggunakan kunci ini harus memilikikms:Decrypt,kms:GenerateDataKey, dan `kms:CreateGrant` izin. Setelah sumber daya dibuat dengan kunci, kunci tidak dapat dihapus atau diubah. Jika Anda menggunakan Kunci yang Dikelola Pelanggan, administrator yang mengakses sumber daya harus memiliki `kms:Decrypt` dan `kms:GenerateDataKey` izin. Jika Anda melihat kesalahan tentang akses ditolak saat menggunakan konsol, pastikan pengguna yang menggunakan konsol memiliki izin ini dengan kunci yang digunakan.

Anda dapat memecahkan masalah dan mengaudit penggunaan kunci dengan memeriksa status hibah. AWS KMS Untuk informasi selengkapnya, lihat Mengelola hibah. Selama pembuatan portal, Browser WorkSpaces Aman membuat hibah untuk memungkinkan layanan mengakses kunci secara asinkron. Anda dapat memeriksa status penggunaan kunci kami dengan memeriksa hibah, serta Konteks Enkripsi yang diberikan saat hibah digunakan. Konteks enkripsi selalu berisi entri dengan kunci `aws:workspaces-web:portal:id` dan nilai yang sama dengan ID portal Anda. Untuk sumber daya lain, konteks enkripsi akan selalu berisi entri dalam format `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` dan ID sumber daya yang sesuai.

Enkripsi bergerak

WorkSpaces Browser Aman mengenkripsi data dalam perjalanan melalui HTTPS dan TLS 1.2. Anda dapat mengirim permintaan WorkSpaces dengan menggunakan konsol atau API panggilan langsung. Data permintaan yang ditransfer dienkripsi dengan mengirimkan semuanya melalui koneksi HTTPS

atau TLS koneksi. Data permintaan dapat ditransfer dari AWS Konsol, AWS Command Line Interface, atau AWS SDK ke Browser WorkSpaces Aman.

Enkripsi dalam transit dikonfigurasi secara default, dan koneksi aman (HTTPS,TLS) dikonfigurasi secara default.

Manajemen kunci

Anda dapat menyediakan Customer Managed AWS KMS Key Anda sendiri untuk mengenkripsi informasi pelanggan Anda. Jika Anda tidak menyediakannya, Browser WorkSpaces Aman akan menggunakan Kunci yang AWS Dimiliki. Anda dapat mengatur kunci Anda menggunakan AWS SDK.

Privasi lalu lintas antar jaringan

Untuk mengamankan koneksi antara Browser WorkSpaces Aman dan aplikasi on-premise, Anda menggunakan Browser WorkSpaces Aman untuk meluncurkan sesi browser di dalam milik Anda sendiri. VPC Koneksi ke aplikasi on-premise dikonfigurasi sendiriVPC, dan tidak dikendalikan oleh WorkSpaces Secure Browser.

Untuk mengamankan koneksi antar akun, WorkSpaces Secure Browser menggunakan peran terkait layanan untuk terhubung dengan aman ke akun pelanggan dan menjalankan operasi atas nama pelanggan. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk WorkSpaces Browser Aman.

Pencatatan akses pengguna

Administrator dapat merekam acara sesi Browser WorkSpaces Aman, termasuk mulai, berhenti, dan URL kunjungan. Log ini dienkripsi dan dikirimkan dengan aman ke pelanggan melalui Amazon Kinesis Data Stream. Informasi penjelajahan dari pencatatan akses pengguna tidak disimpan oleh AWS, atau tersedia dari sesi tanpa pencatatan yang dikonfigurasi. URLkunjungan dalam mode penyamaran, atau dihapus URLs dari riwayat browser, tidak direkam dalam pencatatan akses pengguna.

Identity and Access Management untuk Amazon WorkSpaces Secure Browser

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAMadministrator mengontrol siapa yang

dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Browser WorkSpaces Aman. IAMadalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Amazon WorkSpaces Secure Browser bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces
- AWS kebijakan terkelola untuk Browser WorkSpaces Aman
- Memecahkan masalah identitas dan akses Amazon WorkSpaces Secure Browser
- Menggunakan peran terkait layanan untuk WorkSpaces Browser Aman

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Browser WorkSpaces Aman.

Pengguna layanan — Jika Anda menggunakan layanan Browser WorkSpaces Aman untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Browser WorkSpaces Aman untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Browser WorkSpaces Aman, lihatMemecahkan masalah identitas dan akses Amazon WorkSpaces Secure Browser.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Browser WorkSpaces Aman di perusahaan Anda, Anda mungkin memiliki akses penuh ke Browser WorkSpaces Aman. Tugas Anda adalah menentukan fitur dan sumber daya Browser WorkSpaces Aman mana yang harus diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasarIAM. Untuk mempelajari selengkapnya tentang cara perusahaan Anda dapat menggunakan IAM Browser WorkSpaces Aman, lihatBagaimana Amazon WorkSpaces Secure Browser bekerja dengan IAM.

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Browser WorkSpaces Aman. Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani AWS API permintaan di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor di Panduan AWS IAM Identity Center Pengguna dan Menggunakan otentikasi multi-faktor (MFA) AWS di Panduan Pengguna. IAM

Akun AWS pengguna root

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

untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di IAMPanduan Pengguna.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensi yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat Apa itu Pusat IAM Identitas? dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensi jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari lebih lanjut, lihat Kapan membuat IAM pengguna (bukan peran) di Panduan IAM Pengguna.

IAMperan

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Menggunakan IAM peran di Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin

melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.

- Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.
- Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna

root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

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

Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai jenis kebijakan

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

Bagaimana Amazon WorkSpaces Secure Browser bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Browser WorkSpaces Aman, pelajari IAM fitur apa saja yang tersedia untuk digunakan dengan Browser WorkSpaces Aman.

IAMfitur yang dapat Anda gunakan dengan Amazon WorkSpaces Secure Browser

IAMfitur	WorkSpaces Dukungan Browser Aman
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC(tag dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin prinsipal	Ya

IAMfitur	WorkSpaces Dukungan Browser Aman
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Browser WorkSpaces Aman dan AWS layanan lainnya dengan sebagian besar IAM fitur, lihat AWS layanan yang berfungsi IAM di Panduan IAM Pengguna.

Kebijakan berbasis identitas untuk Browser Aman WorkSpaces

Mendukung kebijakan berbasis identitas: Ya

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

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk Browser Aman WorkSpaces

Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman, lihat. Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Kebijakan berbasis sumber daya dalam Secure Browser WorkSpaces

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya,

administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau IAM entitas di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

Tindakan kebijakan untuk Browser WorkSpaces Aman

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

`Action`Elemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Browser WorkSpaces Aman, lihat Tindakan yang ditentukan oleh Amazon WorkSpaces Secure Browser di Referensi Otorisasi Layanan.

Tindakan kebijakan di Browser WorkSpaces Aman menggunakan awalan berikut sebelum tindakan:

```
workspaces-web
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "workspaces-web:action1",
      "workspaces-web:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman, lihat. Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Sumber daya kebijakan untuk Browser WorkSpaces Aman

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Browser WorkSpaces Aman dan jenisnyaARNs, lihat Sumber daya yang ditentukan oleh Amazon WorkSpaces Secure Browser di Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon WorkSpaces Secure Browser.

Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman, lihat. Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Kunci kondisi kebijakan untuk Browser WorkSpaces Aman

Mendukung kunci kondisi kebijakan khusus layanan: Ya

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

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan IAM Pengguna.

Untuk melihat daftar kunci kondisi Browser WorkSpaces Aman, lihat Kunci kondisi untuk Browser WorkSpaces Aman Amazon di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon WorkSpaces Secure Browser.

Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman, lihat. Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Daftar kontrol akses (ACLs) di Browser WorkSpaces Aman

MendukungACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Kontrol akses berbasis atribut (ABAC) dengan WorkSpaces Browser Aman

Mendukung ABAC (tag dalam kebijakan): Sebagian

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABACmembantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi lebih lanjut tentangABAC, lihat Apa ituABAC? dalam IAMUser Guide. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

Menggunakan kredensi sementara dengan WorkSpaces Browser Aman

Mendukung kredensi sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensil sementara, lihat Layanan AWS yang berfungsi IAM di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih ke peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensi sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensi keamanan sementara di. IAM

Izin utama lintas layanan untuk WorkSpaces Browser Aman

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

Peran layanan untuk Browser WorkSpaces Aman

Mendukung peran layanan: Tidak

Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Browser WorkSpaces Aman. Edit peran layanan hanya jika Browser WorkSpaces Aman memberikan panduan untuk melakukannya.

Peran terkait layanan untuk WorkSpaces Browser Aman

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat AWS layanan yang berfungsi dengannya. IAM Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Browser WorkSpaces Aman. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat Membuat JSON IAM kebijakan di Panduan Pengguna. IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Browser WorkSpaces Aman, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Browser WorkSpaces Aman Amazon di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Browser WorkSpaces Aman
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi API akses MFA yang dilindungi di IAMPanduan Pengguna.

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

Menggunakan konsol Browser WorkSpaces Aman

Untuk mengakses konsol Amazon WorkSpaces Secure Browser, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Browser WorkSpaces Aman di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau. AWS API Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan API operasi yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Browser WorkSpaces Aman, lampirkan juga Browser WorkSpaces Aman `ConsoleAccess` atau kebijakan `ReadOnly` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna di Panduan IAM Pengguna.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan IAM pengguna melihat kebijakan sebaris dan terkelola yang dilampirkan pada identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan atau. AWS CLI AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola untuk Browser WorkSpaces Aman

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di AWS akun Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang dapat menambahkan izin tambahan ke kebijakan AWS terkelola untuk mendukung fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan `ReadOnlyAccess` AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWS kebijakan terkelola: AmazonWorkSpacesWebServiceRolePolicy

Anda tidak dapat melampirkan kebijakan `AmazonWorkSpacesWebServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Browser WorkSpaces Aman melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat the section called “Menggunakan Peran Terkait Layanan”.

Kebijakan ini memberikan izin administratif yang memungkinkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh Browser WorkSpaces Aman.

Detail izin

Kebijakan ini mencakup izin berikut:

- `workspaces-web`— Memungkinkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh Browser WorkSpaces Aman.
- `ec2`— Memungkinkan prinsipal untuk menggambarkan VPC, subnet, dan zona ketersediaan; membuat, menandai, mendeskripsikan, dan menghapus antarmuka jaringan; mengaitkan atau memisahkan alamat; dan menjelaskan tabel rute, grup keamanan, dan titik akhir VPC.
- `CloudWatch`— Memungkinkan kepala sekolah untuk menempatkan data metrik.
- `Kinesis`- Memungkinkan prinsipal untuk menjelaskan ringkasan aliran data Kinesis dan memasukkan catatan ke dalam aliran data Kinesis untuk pencatatan akses pengguna. Untuk informasi selengkapnya, lihat the section called “Siapkan pencatatan akses pengguna”.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
```

```
                        "WorkSpacesWebManaged"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/WorkSpacesWeb",
                        "AWS/Usage"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStreamSummary"
            ],
            "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
        }
    ]
}
```

AWS kebijakan terkelola: AmazonWorkSpacesSecureBrowserReadOnly

Anda dapat melampirkan kebijakan `AmazonWorkSpacesSecureBrowserReadOnly` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan akses ke Browser WorkSpaces Aman dan dependensinya melalui AWS Management Console, SDK, dan CLI. Kebijakan ini tidak menyertakan izin yang diperlukan untuk berinteraksi dengan portal yang digunakan `IAM_Identity_Center` sebagai jenis autentikasi. Untuk mendapatkan izin ini, gabungkan kebijakan ini dengan`AWSSSOReadOnly`.

Detail izin

Kebijakan ini mencakup izin berikut.

- `workspaces-web`— Menyediakan akses read-only ke WorkSpaces Secure Browser dan dependensinya melalui AWS Management Console, SDK, dan CLI.
- `ec2`— Memungkinkan kepala sekolah untuk menggambarkan VPC, subnet, dan kelompok keamanan. Ini digunakan di Konsol AWS Manajemen di Browser WorkSpaces Aman untuk menunjukkan kepada Anda VPC, subnet, dan grup keamanan yang tersedia untuk digunakan dengan layanan.
- `Kinesis`- Memungkinkan kepala sekolah untuk daftar aliran data Kinesis. Ini digunakan di Konsol AWS Manajemen di Browser WorkSpaces Aman untuk menunjukkan aliran data Kinesis yang tersedia untuk digunakan dengan layanan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
```

```
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AmazonWorkSpacesWebReadOnly

Anda dapat melampirkan kebijakan `AmazonWorkSpacesWebReadOnly` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan akses ke Browser WorkSpaces Aman dan dependensinya melalui AWS Management Console, SDK, dan CLI. Kebijakan ini tidak menyertakan izin yang diperlukan untuk berinteraksi dengan portal yang digunakan `IAM_Identity_Center` sebagai jenis autentikasi. Untuk mendapatkan izin ini, gabungkan kebijakan ini dengan`AWSSSOReadOnly`.

> **Note**
>
> Jika saat ini Anda menggunakan kebijakan ini, beralihlah ke `AmazonWorkSpacesSecureBrowserReadOnly` kebijakan baru.

Detail izin

Kebijakan ini mencakup izin berikut.

- `workspaces-web`— Menyediakan akses read-only ke WorkSpaces Secure Browser dan dependensinya melalui AWS Management Console, SDK, dan CLI.
- `ec2`— Memungkinkan kepala sekolah untuk menggambarkan VPC, subnet, dan kelompok keamanan. Ini digunakan di Konsol AWS Manajemen di Browser WorkSpaces Aman untuk menunjukkan kepada Anda VPC, subnet, dan grup keamanan yang tersedia untuk digunakan dengan layanan.
- `Kinesis`- Memungkinkan kepala sekolah untuk daftar aliran data Kinesis. Ini digunakan di Konsol AWS Manajemen di Browser WorkSpaces Aman untuk menunjukkan aliran data Kinesis yang tersedia untuk digunakan dengan layanan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
```

```
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkSpaces Mengamankan pembaruan Browser ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Browser WorkSpaces Aman sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman Riwayat dokumen.

Perubahan	Deskripsi	Tanggal
AmazonWorkSpacesSecureBrowserReadOnly – Kebijakan baru	WorkSpaces Secure Browser menambahkan kebijakan baru untuk menyediakan akses hanya-baca ke WorkSpaces Secure Browser dan dependensinya melalui AWS	24 Juni 2024

Perubahan	Deskripsi	Tanggal
	Management Console, SDK, dan CLI.	
AmazonWorkSpacesWebServiceRolePolicy— Kebijakan yang diperbarui	WorkSpaces Secure Browser memperbarui kebijakan CreateNetworkInterface untuk membatasi tag dengan aws:RequestTag/WorkSpacesWebManaged: true dan bertindak atas sumber daya subnet dan grup keamanan, serta membatasi DeleteNetworkInterface untuk ENI yang ditandai dengan aws:/: true. ResourceTag WorkSpacesWebManaged	Desember 15, 2022
AmazonWorkSpacesWebReadOnly— Kebijakan yang diperbarui	WorkSpaces Browser Aman memperbarui kebijakan untuk menyertakan izin baca untuk pencatatan akses pengguna dan daftar aliran data Kinesis. Untuk informasi selengkapnya, lihat the section called “Siapkan pencatatan akses pengguna”.	2 November 2022

Perubahan	Deskripsi	Tanggal
AmazonWorkSpacesWebServiceRolePolicy— Kebijakan yang diperbarui	WorkSpaces Secure Browser memperbarui kebijakan untuk menjelaskan ringkasan aliran data Kinesis dan memasukkan catatan ke dalam aliran data Kinesis untuk pencatatan akses pengguna. Untuk informasi selengkapnya, lihat the section called “Siapkan pencatatan akses pengguna”.	Oktober 17, 2022
AmazonWorkSpacesWebServiceRolePolicy— Kebijakan yang diperbarui	WorkSpaces Secure Browser memperbarui kebijakan untuk membuat tag selama pembuatan ENI.	September 6, 2022
AmazonWorkSpacesWebServiceRolePolicy— Kebijakan yang diperbarui	WorkSpaces Secure Browser memperbarui kebijakan untuk menambahkan namespace AWS/Usage ke izin API. PutMetricData	April 6, 2022
AmazonWorkSpacesWebReadOnly – Kebijakan baru	WorkSpaces Secure Browser menambahkan kebijakan baru untuk menyediakan akses hanya-baca ke WorkSpaces Secure Browser dan dependensinya melalui AWS Management Console, SDK, dan CLI.	30 November 2021

Perubahan	Deskripsi	Tanggal
AmazonWorkSpacesWebServiceRolePolicy – Kebijakan baru	WorkSpaces Secure Browser menambahkan kebijakan baru untuk mengizinkan akses ke layanan AWS dan sumber daya yang digunakan atau dikelola oleh WorkSpaces Secure Browser.	30 November 2021
WorkSpaces Browser Aman mulai melacak perubahan	WorkSpaces Browser Aman mulai melacak perubahan untuk kebijakan yang AWS dikelola.	30 November 2021

Memecahkan masalah identitas dan akses Amazon WorkSpaces Secure Browser

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Browser WorkSpaces Aman danIAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Browser WorkSpaces Aman
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Browser WorkSpaces Aman saya

Saya tidak berwenang untuk melakukan tindakan di Browser WorkSpaces Aman

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

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

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web:GetWidget on resource: my-example-widget
```

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

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

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Browser WorkSpaces Aman.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Browser WorkSpaces Aman. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

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

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Browser WorkSpaces Aman saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis

sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Browser WorkSpaces Aman mendukung fitur-fitur ini, lihatBagaimana Amazon WorkSpaces Secure Browser bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di Panduan Pengguna. IAM
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

Menggunakan peran terkait layanan untuk WorkSpaces Browser Aman

Amazon WorkSpaces Secure Browser menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke WorkSpaces Browser Aman. Peran terkait layanan telah ditentukan sebelumnya oleh Browser WorkSpaces Aman dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Browser WorkSpaces Aman lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. WorkSpaces Secure Browser mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya WorkSpaces Secure Browser yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan izin. Kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini melindungi sumber daya Browser WorkSpaces Aman Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait

Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Browser Aman WorkSpaces

WorkSpaces Secure Browser menggunakan peran terkait layanan bernama `AWSServiceRoleForAmazonWorkSpacesWeb` — WorkSpaces Secure Browser menggunakan peran terkait layanan ini untuk mengakses sumber daya Amazon EC2 dari akun pelanggan untuk streaming instans dan metrik. CloudWatch

`AWSServiceRoleForAmazonWorkSpacesWeb` peran terkait layanan memercayakan layanan berikut untuk menjalankan peran tersebut:

- `workspaces-web.amazonaws.com`

Kebijakan izin peran bernama `AmazonWorkSpacesWebServiceRolePolicy` memungkinkan Browser WorkSpaces Aman untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan. Untuk informasi selengkapnya, lihat the section called "AmazonWorkSpacesWebServiceRolePolicy".

- Tindakan: `ec2:DescribeVpcs` pada `all AWS resources`
- Tindakan: `ec2:DescribeSubnets` pada `all AWS resources`
- Tindakan: `ec2:DescribeAvailabilityZones` pada `all AWS resources`
- Tindakan: `ec2:CreateNetworkInterface` dengan `aws:RequestTag/WorkSpacesWebManaged: true` sumber daya subnet dan grup keamanan
- Tindakan: `ec2:DescribeNetworkInterfaces` pada `all AWS resources`
- Tindakan: `ec2:DeleteNetworkInterface` pada antarmuka jaringan dengan `aws:ResourceTag/WorkSpacesWebManaged: true`
- Tindakan: `ec2:DescribeSubnets` pada `all AWS resources`
- Tindakan: `ec2:AssociateAddress` pada `all AWS resources`
- Tindakan: `ec2:DisassociateAddress` pada `all AWS resources`
- Tindakan: `ec2:DescribeRouteTables` pada `all AWS resources`
- Tindakan: `ec2:DescribeSecurityGroups` pada `all AWS resources`
- Tindakan: `ec2:DescribeVpcEndpoints` pada `all AWS resources`

- Tindakan: `ec2:CreateTags` pada `ec2:CreateNetworkInterface` Operasi dengan `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Tindakan: `cloudwatch:PutMetricData` pada `all AWS resources`
- Tindakan: `kinesis:PutRecord` pada aliran data Kinesis dengan nama yang dimulai dengan `amazon-workspaces-web-`
- Tindakan: `kinesis:PutRecords` pada aliran data Kinesis dengan nama yang dimulai dengan `amazon-workspaces-web-`
- Tindakan: `kinesis:DescribeStreamSummary` pada aliran data Kinesis dengan nama yang dimulai dengan `amazon-workspaces-web-`

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk WorkSpaces Browser Aman

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat portal pertama di, API AWS Management Console, atau AWS API AWS CLI, WorkSpaces Secure Browser akan membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini.

Jika Anda menghapus peran terkait layanan ini dan kemudian perlu membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran di akun Anda. Saat Anda membuat portal pertama, WorkSpaces Secure Browser akan membuat peran terkait layanan untuk Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan Browser WorkSpaces Aman. Di AWS CLI atau AWS API, buat peran terkait layanan dengan nama `workspaces-web.amazonaws.com` layanan. Untuk informasi lebih lanjut, lihat Membuat Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait layanan untuk WorkSpaces Browser Aman

WorkSpaces Browser Aman tidak memungkinkan Anda mengedit peran `AWSServiceRoleForAmazonWorkSpacesWeb` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Browser Aman WorkSpaces

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Browser WorkSpaces Aman menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya Browser WorkSpaces Aman yang digunakan oleh AWSServiceRoleForAmazonWorkSpacesWeb

- Pilih dari salah satu opsi berikut:
  - Jika Anda menggunakan konsol, hapus semua portal Anda di konsol.
  - Jika Anda menggunakan CLI atau API, lepaskan semua sumber daya Anda (termasuk pengaturan browser, pengaturan jaringan, pengaturan pengguna, penyimpanan kepercayaan, dan pengaturan pencatatan akses pengguna) dari portal Anda, hapus sumber daya ini, lalu hapus portal.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForAmazonWorkSpacesWeb terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran WorkSpaces terkait layanan Browser Aman

WorkSpaces Secure Browser mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Wilayah dan Titik Akhir AWS.

Respons insiden di Amazon WorkSpaces Secure Browser

Anda dapat mendeteksi insiden dengan memantau CloudWatch metrik `SessionFailure` Amazon. Untuk menerima peringatan untuk insiden, gunakan CloudWatch alarm untuk metrik. `SessionFailure` Untuk informasi selengkapnya, lihat Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch.

Validasi kepatuhan untuk Amazon WorkSpaces Secure Browser

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk HIPAA Keamanan dan Kepatuhan di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat HIPAA aplikasi yang memenuhi syarat.

  > **Note**
  >
  > Tidak semua Layanan AWS HIPAA memenuhi syarat. Untuk informasi selengkapnya, lihat Referensi Layanan yang HIPAA Memenuhi Syarat.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.

- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi ()). ISO
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCIDSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Browser Aman Amazon WorkSpaces

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Berikut ini saat ini tidak didukung oleh Browser WorkSpaces Aman:

- Mencadangkan konten di seluruh AZ atau wilayah
- Cadangan terenkripsi
- Mengenkripsi konten dalam perjalanan antara AZ atau wilayah
- Pencadangan default atau otomatis

Untuk mengonfigurasi ketersediaan internet yang tinggi, Anda dapat menyetel konfigurasi VPC Anda. Untuk ketersediaan API yang tinggi, Anda dapat meminta jumlah TPS yang tepat.

Keamanan infrastruktur di Amazon WorkSpaces Secure Browser

Sebagai layanan terkelola, Amazon WorkSpaces Secure Browser dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan API panggilan yang AWS dipublikasikan untuk mengakses Amazon WorkSpaces Secure Browser melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

WorkSpaces Browser Aman mengisolasi lalu lintas layanan dengan menerapkan Otentikasi dan Otorisasi AWS SigV4 Standar ke semua layanan. Titik akhir sumber daya pelanggan (atau titik akhir portal web) dilindungi oleh penyedia identitas Anda. Anda dapat mengisolasi lalu lintas lebih lanjut dengan menggunakan Otorisasi Multi-faktor dan mekanisme keamanan lainnya di penyedia identitas Anda (IDP).

Semua akses internet dapat dikontrol dengan mengkonfigurasi pengaturan jaringan, seperti subnetVPC, atau grup keamanan. Multi-tenancy dan VPC endpoint (PrivateLink) saat ini tidak didukung.

Analisis konfigurasi dan kerentanan di Amazon WorkSpaces Secure Browser

WorkSpaces Pembaruan Browser Aman dan tambalan aplikasi dan platform sesuai kebutuhan atas nama Anda, termasuk Chrome dan Linux. Anda tidak diharuskan untuk menambal atau membangun kembali. Namun, Anda bertanggung jawab untuk mengonfigurasi Browser WorkSpaces Aman sesuai dengan spesifikasi dan pedoman, dan untuk memantau penggunaan Browser WorkSpaces Aman oleh pengguna Anda. Semua konfigurasi terkait layanan dan analisis kerentanan adalah tanggung jawab Secure Browser. WorkSpaces

Anda dapat meminta peningkatan batas untuk sumber daya Browser WorkSpaces Aman, seperti jumlah portal web dan jumlah pengguna. WorkSpaces Browser Aman memastikan ketersediaan layanan dan SLA.

Praktik terbaik keamanan untuk Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser menyediakan sejumlah fitur keamanan yang dapat Anda gunakan saat mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

Praktik terbaik untuk Amazon WorkSpaces Secure Browser mencakup hal-hal berikut:

- Untuk mendeteksi potensi peristiwa keamanan yang terkait dengan penggunaan Browser WorkSpaces Aman, gunakan AWS CloudTrail atau Amazon CloudWatch untuk mendeteksi dan melacak riwayat akses dan log proses. Untuk informasi selengkapnya, lihat Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch dan Mencatat panggilan API Browser WorkSpaces Aman menggunakan AWS CloudTrail.
- Untuk menerapkan kontrol detektif dan mengidentifikasi anomali, gunakan CloudTrail log dan metrik. CloudWatch Untuk informasi selengkapnya, lihat Memantau Browser WorkSpaces Aman

Amazon dengan Amazon CloudWatch dan Mencatat panggilan API Browser WorkSpaces Aman menggunakan AWS CloudTrail.

- Anda dapat mengatur pencatatan akses pengguna untuk merekam peristiwa pengguna. Untuk informasi selengkapnya, lihat the section called “Siapkan pencatatan akses pengguna”.

Untuk mencegah potensi peristiwa keamanan yang terkait dengan penggunaan Browser WorkSpaces Aman oleh Anda, ikuti praktik terbaik berikut ini:

- Terapkan akses hak istimewa paling sedikit dan buat peran khusus yang akan digunakan untuk tindakan Browser WorkSpaces Aman. Gunakan templat IAM untuk membuat peran Akses Penuh atau Hanya Baca. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk Browser WorkSpaces Aman.
- Hati-hati dengan berbagi domain portal dan kredensi pengguna. Siapa pun di internet dapat mengakses portal web, tetapi mereka tidak dapat memulai sesi kecuali mereka memiliki kredensi pengguna yang valid ke portal. Berhati-hatilah tentang bagaimana, kapan, dan kepada siapa Anda berbagi kredensi portal web.

Memantau Peramban WorkSpaces Aman Amazon

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon WorkSpaces Secure Browser dan AWS solusi Anda lainnya. AWS menyediakan alat pemantauan berikut untuk menonton portal Browser WorkSpaces Aman Anda dan sumber dayanya, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan menyetel alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat CloudWatch melacak penggunaan CPU atau metrik lain untuk instans Amazon EC2 Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari instans Amazon EC2 CloudTrail, dan sumber lainnya. CloudWatch Log dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang batas tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS CloudTrail.

Topik

- Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch
- Mencatat panggilan API Browser WorkSpaces Aman menggunakan AWS CloudTrail
- Pencatatan akses pengguna

Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch

Anda dapat memantau Amazon WorkSpaces Secure Browser menggunakan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati real-time. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Namespace `AWS/WorkSpacesWeb` mencakup metrik berikut.

CloudWatch metrik untuk Amazon WorkSpaces Secure Browser

Metrik	Deskripsi	Dimensi	Statistik	Unit
`SessionAttempt`	Jumlah upaya sesi Amazon WorkSpaces Secure Browser.	`PortalId`	Rata-rata, Jumlah, Maksimum, Minimum	Hitung
`SessionSuccess`	Jumlah sesi Amazon WorkSpaces Secure Browser yang sukses dimulai.	`PortalId`	Rata-rata, Jumlah, Maksimum, Minimum	Hitung
`SessionFailure`	Jumlah sesi Amazon WorkSpaces Secure Browser yang gagal dimulai.	`PortalId`	Rata-rata, Jumlah, Maksimum, Minimum	Hitung
`GlobalCpuPercent`	Penggunaan CPU dari	`PortalId`	Rata-rata, Jumlah,	Persen

Metrik	Deskripsi	Dimensi	Statistik	Unit
	instance sesi Amazon WorkSpaces Secure Browser.		Maksimum, Minimum	
`GlobalMemoryPercent`	Penggunaan memori (RAM) dari instance sesi Amazon WorkSpaces Secure Browser.	`PortalId`	Rata-rata, Jumlah, Maksimum, Minimum	Persen

> **Note**
>
> Anda dapat melihat statistik metrik “SampleCount” untuk `GlobalCpuPercent` atau `GlobalMemoryPercent` untuk menentukan jumlah sesi bersamaan yang aktif di portal Anda. Titik data dipancarkan oleh setiap sesi sekali per menit.

Mencatat panggilan API Browser WorkSpaces Aman menggunakan AWS CloudTrail

WorkSpaces Secure Browser terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon WorkSpaces Secure Browser. CloudTrail menangkap semua panggilan API untuk Amazon WorkSpaces Secure Browser sebagai peristiwa. Ini termasuk panggilan dari konsol Amazon WorkSpaces Secure Browser dan panggilan kode ke operasi Amazon WorkSpaces Secure Browser API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Amazon WorkSpaces Secure Browser. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat mengidentifikasi permintaan yang dibuat ke Amazon WorkSpaces Secure Browser, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, serta detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

WorkSpaces Amankan informasi Browser di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Saat aktivitas terjadi di Amazon WorkSpaces Secure Browser, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Dalam riwayat acara, Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Amazon WorkSpaces Secure Browser, Anda dapat membuat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua tindakan Amazon WorkSpaces Secure Browser dicatat oleh CloudTrail dan didokumentasikan dalam Referensi WorkSpaces API Amazon. Misalnya, panggilan ke`CreatePortal`, `DeleteUserSettings` dan `ListBrowserSettings` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan tersebut dibuat dengan kredensial root atau pengguna IAM.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.

Memahami entri file log Browser WorkSpaces Aman

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili satu permintaan dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan detail lainnya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `ListBrowserSettings` tindakan.


```
{
   "Records": [{
       "eventVersion": "1.08",
       "userIdentity": {
           "type": "IAMUser",
           "principalId": "111122223333",
           "arn": "arn:aws:iam::111122223333:user/myUserName",
           "accountId": "111122223333",
           "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
           "userName": "myUserName"
       },
       "eventTime": "2021-11-17T23:44:51Z",
       "eventSource": "workspaces-web.amazonaws.com",
       "eventName": "ListBrowserSettings",
       "awsRegion": "us-west-2",
       "sourceIPAddress": "127.0.0.1",
       "userAgent": "[]",
       "requestParameters": null,
       "responseElements": null,
       "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
       "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
       "readOnly": true,
       "eventType": "AwsApiCall",
       "managementEvent": true,
       "recipientAccountId": "111122223333",
       "eventCategory": "Management"
   },
```

```
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2021-11-17T23:55:51Z",
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "CreateUserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "5127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "clientToken": "some-token",
            "copyAllowed": "Enabled",
            "downloadAllowed": "Enabled",
            "pasteAllowed": "Enabled",
            "printAllowed": "Enabled",
            "uploadAllowed": "Enabled"
        },
        "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
        "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
        "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    }]
}
```

Pencatatan akses pengguna

Amazon WorkSpaces Secure Browser memungkinkan pelanggan merekam acara sesi, termasuk memulai, berhenti, dan kunjungan URL. Log ini dikirimkan ke Amazon Kinesis Data Stream yang

Anda tentukan untuk portal web Anda. Untuk informasi selengkapnya, lihat the section called “Siapkan pencatatan akses pengguna”.

Panduan untuk pengguna Browser WorkSpaces Aman

Administrator menggunakan Browser WorkSpaces Aman untuk membuat portal web yang terhubung ke situs web perusahaan, seperti situs web internal, aplikasi web software-as-a-service (SAAS), atau internet. Pengguna akhir menggunakan browser web mereka yang ada untuk mengakses portal web ini untuk meluncurkan sesi dan mengakses konten.

Konten berikut membantu memandu pengguna akhir yang ingin mempelajari lebih lanjut tentang mengakses Browser WorkSpaces Aman, meluncurkan dan mengonfigurasi sesi, serta menggunakan bilah alat dan browser web.

Topik

- Kompatibilitas browser dan perangkat
- Akses portal web
- Bimbingan sesi
- Pemecahan Masalah
- Ekstensi untuk sistem masuk tunggal

Kompatibilitas browser dan perangkat

Amazon WorkSpaces Secure Browser didukung oleh klien browser web NICE DCV, yang berjalan di dalam browser web, jadi tidak diperlukan instalasi. Klien browser web didukung oleh browser web umum, seperti Chrome dan Firefox, dan oleh sistem operasi desktop utama, seperti Windows, macOS, dan Linux.

Untuk up-to-date detail paling detail tentang dukungan klien browser web, lihat Klien browser Web.

> **Note**
>
> Support untuk webcam saat ini hanya tersedia di browser berbasis Chromium, seperti Google Chrome dan Microsoft Edge. Saat ini, Apple Safari dan Mozilla FireFox tidak mendukung webcam.

Akses portal web

Administrator Anda dapat memberikan akses ke portal web Anda dengan opsi berikut:

- Anda dapat memilih tautan dari email atau situs web, lalu masuk dengan kredensil identitas SAMP Anda.
- Anda dapat masuk ke penyedia identitas SAMP Anda (seperti Okta, Ping, atau Azure), dan meluncurkan sesi dengan satu klik dari halaman beranda aplikasi penyedia SAMP Anda (seperti Okta End User Dashboard atau portal Azure Myapps).

Bimbingan sesi

Setelah Anda masuk ke portal web, Anda dapat meluncurkan sesi dan melakukan berbagai tindakan selama sesi Anda.

Topik

- Mulai sesi
- Gunakan toolbar
- Gunakan browser
- Mengakhiri sesi

Mulai sesi

Setelah Anda masuk untuk meluncurkan sesi, Anda akan melihat pesan sesi peluncuran dan bilah kemajuan. Ini menunjukkan bahwa Amazon WorkSpaces Secure Browser membuat sesi untuk Anda. Di belakang layar, Amazon WorkSpaces Secure Browser membuat instance, meluncurkan browser web terkelola, dan menerapkan pengaturan administrator dan kebijakan browser.

Jika ini adalah pertama kalinya Anda masuk ke portal web Anda, Anda akan melihat ikon biru + di bilah alat. Ikon ini menunjukkan bahwa tutorial tersedia, yang akan memandu melalui fitur yang tersedia di toolbar. Anda dapat menggunakan ikon ini untuk mempelajari cara:

- Izinkan izin browser untuk mikrofon, webcam, dan clipboard, dengan memilih ikon kunci di sebelah browser lokal Anda, dan mengatur sakelar ke Aktif di sebelah clipboard, mikrofon, dan kamera.

> **Note**
>
> Saat Anda mengaktifkan izin webcam di awal sesi pertama Anda, webcam diaktifkan sebentar dan lampu di komputer Anda akan berkedip. Ini memberikan akses browser lokal ke webcam Anda.

- Aktifkan Amazon WorkSpaces Secure Browser untuk meluncurkan jendela monitor tambahan, dengan memilih ikon kunci di browser Anda dan pengaturan untuk Selalu izinkan pop-up.

Jika Anda ingin meluncurkan kembali tutorial, Anda dapat memilih Profil dari toolbar, Help, dan Launch tutorial.

Gunakan toolbar

Untuk memindahkan bilah alat, pilih bilah yang lebih ringan di bagian atas bilah alat, seret ke lokasi yang Anda inginkan, lalu lepaskan untuk menjatuhkannya.

Untuk menutup bilah alat, arahkan kursor ke atasnya, dan pilih tombol panah atas, atau klik dua kali bilah yang lebih ringan di bagian atas. Tampilan yang diciutkan memberi Anda lebih banyak real estat layar, dan akses satu klik ke ikon yang paling umum digunakan.

Untuk menambah ukuran layar, pilih jendela browser dan perbesar. Untuk meningkatkan ukuran tampilan ikon bilah alat dan teks, pilih bilah alat dan perbesar.

Untuk memperbesar atau memperkecil perangkat Windows, ikuti langkah-langkah berikut:

1. Pilih toolbar atau konten web.
2. Tekan Ctrl++ untuk memperbesar, atau tekan Ctrl + - untuk memperkecil.

Untuk memperbesar atau memperkecil perangkat Mac, ikuti langkah-langkah berikut:

1. Pilih toolbar atau konten web.
2. Tekan Cmd ++ untuk memperbesar, atau tekan Cmd + - untuk memperkecil.

Untuk memasang toolbar ke bagian atas layar, pilih Preferences, General, dan Docked di bawah mode Toolbar.

Tabel berikut mencakup deskripsi semua ikon yang tersedia di toolbar:

Icon	Title	Description
	**Windows**	Move between windows or launch additional browser windows.
	**Launch additional monitor window**	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	**Full screen**	Launch a full screen experience view.
	**Microphone**	Activate mic input for the session.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	**Notifications**	Get one-click access to session notifications.
	**Clipboard**	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	**Files**	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.

> **Note**
>
> Ikon Clipboard dan File disembunyikan secara default, kecuali administrator Anda memberikan izin ini. Hanya administrator yang dapat mengaktifkan atau menonaktifkan clipboard dan file di portal web. Jika ikon ini disembunyikan dan Anda perlu mengaksesnya, hubungi administrator Anda.

Gunakan browser

Ketika Anda memulai sesi Anda, browser menampilkan URL Startup, yang merupakan URL yang dipilih oleh administrator Anda. Jika administrator belum memilih URL Startup, Anda akan melihat pengalaman tab baru default dari Google Chrome.

Dari browser, Anda dapat membuka tab, meluncurkan jendela browser tambahan (dari ikon toolbar Windows atau menu triple dot browser), memasukkan URL atau mencari di bilah URL, atau pergi ke situs web dari bookmark terkelola. Untuk mengakses bookmark untuk portal web, buka folder Bookmark Terkelola di bilah bookmark (di bawah bilah URL), atau buka pengelola bookmark dari menu titik tiga di sisi kanan bilah URL.

Untuk mengubah ukuran atau memindahkan jendela browser, seret ke bawah strip tab Chrome. Ini memungkinkan lebih banyak real estat layar untuk beberapa jendela browser selama sesi.

> **Note**
>
> Fitur browser, seperti mode Penyamaran, mungkin tidak tersedia selama sesi Anda jika administrator Anda telah mematikannya.

Mengakhiri sesi

Untuk mengakhiri sesi, pilih Profil dan Akhir sesi. Setelah sesi berakhir, Amazon WorkSpaces Secure Browser menghapus semua data dari sesi. Tidak ada data browser, seperti situs web terbuka atau riwayat, atau file atau data dari File Explorer yang tersedia setelah sesi berakhir.

Jika Anda menutup tab selama sesi aktif, sesi berakhir setelah periode waktu yang ditetapkan oleh administrator Anda. Jika Anda menutup tab dan mengunjungi kembali portal web sebelum batas waktu ini berlaku, Anda dapat bergabung dengan sesi saat ini dan melihat semua data sesi Anda sebelumnya, seperti membuka situs web dan file.

Pemecahan Masalah

Portal Browser WorkSpaces Aman Amazon saya tidak mengizinkan saya masuk. Saya menerima pesan kesalahan yang mengatakan "Portal web Anda belum diatur. Hubungi administrator TI Anda untuk bantuan. “

Administrator Anda harus menyelesaikan pembuatan portal dengan penyedia identitas SAMP 2.0 agar Anda dapat masuk. Hubungi administrator Anda untuk bantuan.

Portal saya tidak akan meluncurkan sesi. Saya menerima pesan kesalahan yang mengatakan” Gagal memesan sesi. Ada kesalahan internal. Silakan coba lagi. “

Ada masalah dengan peluncuran sesi portal web Anda. Coba luncurkan sesi lagi. Jika ini berlanjut, hubungi administrator Anda untuk bantuan.

Saya tidak bisa menggunakan clipboard, mikrofon, atau webcam.

Untuk mengizinkan izin browser, pilih ikon kunci di sebelah URL, dan alihkan sakelar biru di sebelah Clipboard, Mikrofon, Kamera, dan Pop-up dan pengalihan untuk mengaktifkan fitur ini.

> **Note**
>
> Jika browser web Anda tidak mendukung input video atau audio, opsi ini tidak akan muncul di bilah alat.

Amazon WorkSpaces Secure Browser real-time audio-video (AV) mengalihkan video webcam lokal dan input audio mikrofon ke sesi streaming browser. Dengan cara ini, Anda dapat menggunakan perangkat lokal Anda untuk konferensi video dan audio dalam sesi streaming Anda dengan browser web berbasis Chromium, seperti Google Chrome atau Microsoft Edge. Webcam saat ini tidak didukung di browser non-Chromium.

Untuk informasi tentang cara mengonfigurasi Google Chrome, lihat Menggunakan kamera & mikrofon.

Portal web saya tidak akan meluncurkan jendela monitor tambahan.

Jika Anda mencoba meluncurkan monitor ganda dan melihat ikon Pop-up diblokir di akhir bilah alamat di browser atas, pilih ikon dan tombol radio di sebelah Selalu izinkan pop-up dan pengalihan.

Dengan pop-up yang diizinkan, pilih ikon Monitor ganda pada bilah alat untuk meluncurkan jendela baru, memposisikan ulang jendela pada monitor Anda, dan seret tab browser ke jendela.

Ketika saya mencoba mengunduh file dari panel File, tidak ada yang terjadi.

Jika Anda mencoba mengunduh file dari panel File dan melihat ikon Pop-up diblokir di akhir bilah alamat di browser atas, pilih ikon dan tombol radio di samping Selalu izinkan pop-up dan pengalihan. Dengan pop-up diizinkan, coba unduh file lagi.

Ekstensi untuk sistem masuk tunggal

Amazon WorkSpaces Secure Browser menawarkan ekstensi untuk sistem masuk tunggal dengan browser Chrome dan Firefox di komputer desktop. Jika administrator Anda telah mengaktifkan ekstensi, portal web akan meminta Anda untuk menginstal ekstensi saat Anda masuk.

Amazon WorkSpaces Secure Browser membuat ekstensi untuk mengaktifkan sistem masuk tunggal ke situs web selama sesi Anda. Misalnya, jika Anda masuk ke portal web Anda menggunakan penyedia identitas SAMP 2.0 (seperti Okta atau Ping), dan Anda mengunjungi situs web selama sesi Anda yang menggunakan penyedia identitas yang sama, ekstensi dapat mempermudah akses situs web dengan menghapus permintaan masuk tambahan.

Anda tidak diharuskan untuk menginstal ekstensi untuk mengakses portal web Anda, tetapi dapat meningkatkan pengalaman Anda dengan mengurangi berapa kali Anda diminta untuk memasukkan nama pengguna dan kata sandi Anda.

Saat Anda masuk, ekstensi akan menempatkan cookie yang terdaftar administrator Anda untuk sesi Anda. Semua data yang ditempatkan ekstensi dienkripsi saat istirahat dan selama transit. Tak satu pun dari data ini disimpan di browser lokal Anda. Saat Anda mengakhiri sesi, semua data sesi Anda (seperti tab terbuka, file yang diunduh, dan cookie yang dikirim ke atau dibuat selama sesi) dihapus.

Kompatibilitas

Ekstensi berfungsi dengan perangkat berikut:

- Laptop
- Komputer desktop

Ekstensi ini berfungsi dengan browser berikut:

- Chrome
- Firefox

Penginstalan

Saat Anda masuk ke portal, ikuti prompt untuk menginstal ekstensi untuk browser Chrome atau Firefox Anda. Anda hanya perlu melakukan ini satu kali untuk setiap browser web.

Jika Anda beralih perangkat, beralih ke browser lain di perangkat yang sama, atau menghapus ekstensi dari browser lokal, Anda akan melihat prompt untuk menginstal ekstensi saat memulai sesi berikutnya.

Untuk memastikan bahwa ekstensi berfungsi seperti yang diharapkan, gunakan ekstensi di jendela penelusuran normal, alih-alih Penyamaran (Chrome) atau Penjelajahan Pribadi (Firefox).

Pemecahan Masalah

Jika ekstensi telah diinstal, tetapi Anda masih diminta untuk masuk selama sesi, ikuti langkah-langkah berikut:

1. Pastikan bahwa Anda memiliki ekstensi Amazon WorkSpaces Secure Browser diinstal pada browser Anda. Jika Anda menghapus data browser Anda, Anda mungkin telah menghapus ekstensi secara tidak sengaja.
2. Pastikan Anda bukan Incognito (Chrome) atau Private Browsing (Firefox). Mode ini dapat menyebabkan masalah dengan ekstensi.
3. Jika masalah berlanjut, hubungi administrator portal Anda untuk bantuan tambahan.

Riwayat dokumen untuk Panduan Administrasi Browser WorkSpaces Aman Amazon

Tabel berikut menjelaskan rilis dokumentasi untuk Amazon WorkSpaces Secure Browser.

Perubahan	Deskripsi	Tanggal
Izinkan tautan dalam	Izinkan portal menerima tautan dalam yang menghubungkan pengguna ke situs web tertentu selama sesi berlangsung.	Juni 25, 2024
Pembaruan kebijakan terkelola	Ditambahkan kebijakan AmazonWorkSpacesSecureBrowserReadOnly terkelola	Juni 24, 2024
Gunakan bilah alat untuk memperbesar	Anda dapat meningkatkan ukuran tampilan, ikon, dan teks dengan bilah alat.	1 Mei 2024
Pengaturan portal web baru	Sekarang Anda dapat menentukan jenis Instance dan batas pengguna bersamaan Max untuk portal web Anda.	April 22, 2024
CloudWatch metrik	Ditambahkan GlobalCpuPercent dan GlobalMemoryPercent metrik.	Februari 26, 2024
Mengatur pemfilteran URL	Anda dapat menggunakan Kebijakan Chrome untuk memfilter URL mana yang dapat diakses pengguna dari browser jarak jauh mereka.	Februari 21, 2024

Jenis otentikasi IDP	Anda dapat memilih jenis otentikasi standar atau IAM Identity Center.	Februari 5, 2024
Aktifkan ekstensi untuk sistem masuk tunggal	Anda dapat mengaktifkan ekstensi agar pengguna akhir Anda memiliki pengalaman masuk portal yang lebih baik.	28 Agustus 2023
Panduan pengguna untuk Amazon WorkSpaces Secure Browser	Menambahkan konten untuk membantu memandu pengguna akhir, yang ingin mempelajari lebih lanjut tentang mengakses Amazon WorkSpaces Secure Browser, meluncurkan dan mengonfig urasi sesi, serta menggunakan bilah alat dan browser web.	Juli 17, 2023
Kontrol akses IP	WorkSpaces Secure Browser memungkinkan Anda mengontrol alamat IP mana portal web Anda dapat diakses.	31 Mei 2023
Pembaruan kebijakan terkelola	Kebijakan AmazonWor kSpacesWebReadOnly terkelola yang diperbarui	15 Mei 2023
Konfigurasikan pembaruan penyedia identitas	WorkSpaces Secure Browser menawarkan dua jenis otentikasi: Standar dan AWS IAM Identity Center	15 Maret 2023
Pembaruan kebijakan browser	Bagian kebijakan browser yang diperbarui dan direstruk turisasi	31 Januari 2023

Pembaruan kebijakan terkelola	Kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola yang diperbarui	Desember 15, 2022
Daftar Izinkan dan Daftar Blokir	Tentukan Allowlist dan Blocklist untuk menentukan daftar domain yang dapat atau tidak dapat diakses oleh pengguna Anda.	November 14, 2022
Pembaruan kebijakan terkelola	Kebijakan AmazonWorkSpacesWebReadOnly terkelola yang diperbarui	2 November 2022
Pembaruan kebijakan terkelola	Kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola yang diperbarui	24 Oktober 2022
Pencatatan akses pengguna	Siapkan pencatatan akses pengguna untuk merekam peristiwa pengguna	Oktober 17, 2022
Pembaruan jaringan	Berbagai pembaruan ke bagian “Jaringan dan akses”	September 22, 2022
Pembaruan kebijakan terkelola	Kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola yang diperbarui	September 6, 2022
Konfigurasikan sesi pengguna	Konfigurasikan Input Method Editor (IME) dan lokalisasi dalam sesi	28 Juli 2022
Pembaruan jaringan	Berbagai pembaruan ke bagian “Jaringan dan akses”	Juli 7, 2022

Nilai batas waktu	Tentukan batas waktu Putuskan sambungan dalam hitungan menit dan batas waktu putuskan sambungan Idle dalam hitungan menit	Mei 16, 2022
Kebijakan terkelola yang diperbarui	Memperbarui kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola untuk menambahkan namespace AWS/Usage ke izin API PutMetricData	April 6, 2022
Peran terkait layanan	AWSServiceRoleForAmazonWorkSpacesWeb Peran terkait layanan baru	30 November 2021
Kebijakan terkelola	Kebijakan AmazonWorkSpacesWebReadOnly terkelola baru	30 November 2021
Kebijakan terkelola	Kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola baru	30 November 2021
Rilis awal	Rilis awal Panduan Administrasi Browser WorkSpaces Aman	30 November 2021

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