aws

Panduan Administrasi

WorkSpaces Web Amazon

WorkSpaces Web Amazon: Panduan Administrasi

Table of Contents

Apa itu Amazon WorkSpaces Web?

Amazon WorkSpaces Web adalah layanan berbasis Linux berdasarkan permintaan, dikelola sepenuhnya, yang dirancang untuk memfasilitasi akses browser yang aman ke situs web internal dan aplikasi software-as-a-service (SaaS). Akses layanan dari browser web yang ada, tanpa beban administrasi manajemen infrastruktur, perangkat lunak klien khusus, atau solusi jaringan pribadi virtual (VPN).

Topik

Istilah yang perlu diketahui saat menggunakan WorkSpaces Web

Untuk membantu Anda memulai dengan WorkSpaces Web, Anda harus terbiasa dengan konsep berikut.

penyedia identitas (IdP)

Penyedia identitas memverifikasi kredensi pengguna Anda. Kemudian mengeluarkan pernyataan otentikasi untuk menyediakan akses ke penyedia layanan. Anda dapat mengkonfigurasi IdP yang ada untuk bekerja dengan WorkSpaces Web.

Proses untuk mengkonfigurasi 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 bagi pengguna Anda untuk menggunakan WorkSpaces Web di IdP Anda.

Dokumen metadata penyedia identitas (IdP)

WorkSpaces Web memerlukan metadata khusus dari penyedia identitas (IdP) Anda. Anda dapat menambahkan metadata ini ke WorkSpaces Web dengan mengunggah file pertukaran metadata yang diunduh dari IdP Anda.

Penyedia layanan (SP)

Penyedia layanan menerima pernyataan otentikasi dan menyediakan layanan kepada pengguna. WorkSpaces Web 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.

Virtual Private Cloud (VPC)

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

Subnet harus memiliki koneksi yang stabil ke internet, dan VPC dan subnet juga harus memiliki koneksi yang stabil ke situs web internal dan Software as a Service (SaaS) bagi pengguna untuk mengakses sumber daya ini.

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

Toko kepercayaan

Jika pengguna yang mengakses situs web melalui WorkSpaces Web 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 menginstal sertifikat tertentu untuk memuat situs web, Anda harus menambahkan sertifikat itu ke toko kepercayaan Anda untuk memungkinkan pengguna mengakses situs tersebut di WorkSpaces Web.

Situs web yang dapat diakses publik biasanya tidak memerlukan perubahan apa pun pada 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 kenaikan batas lebih dari satu portal, hubungi dukungan.

Titik akhir portal web

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

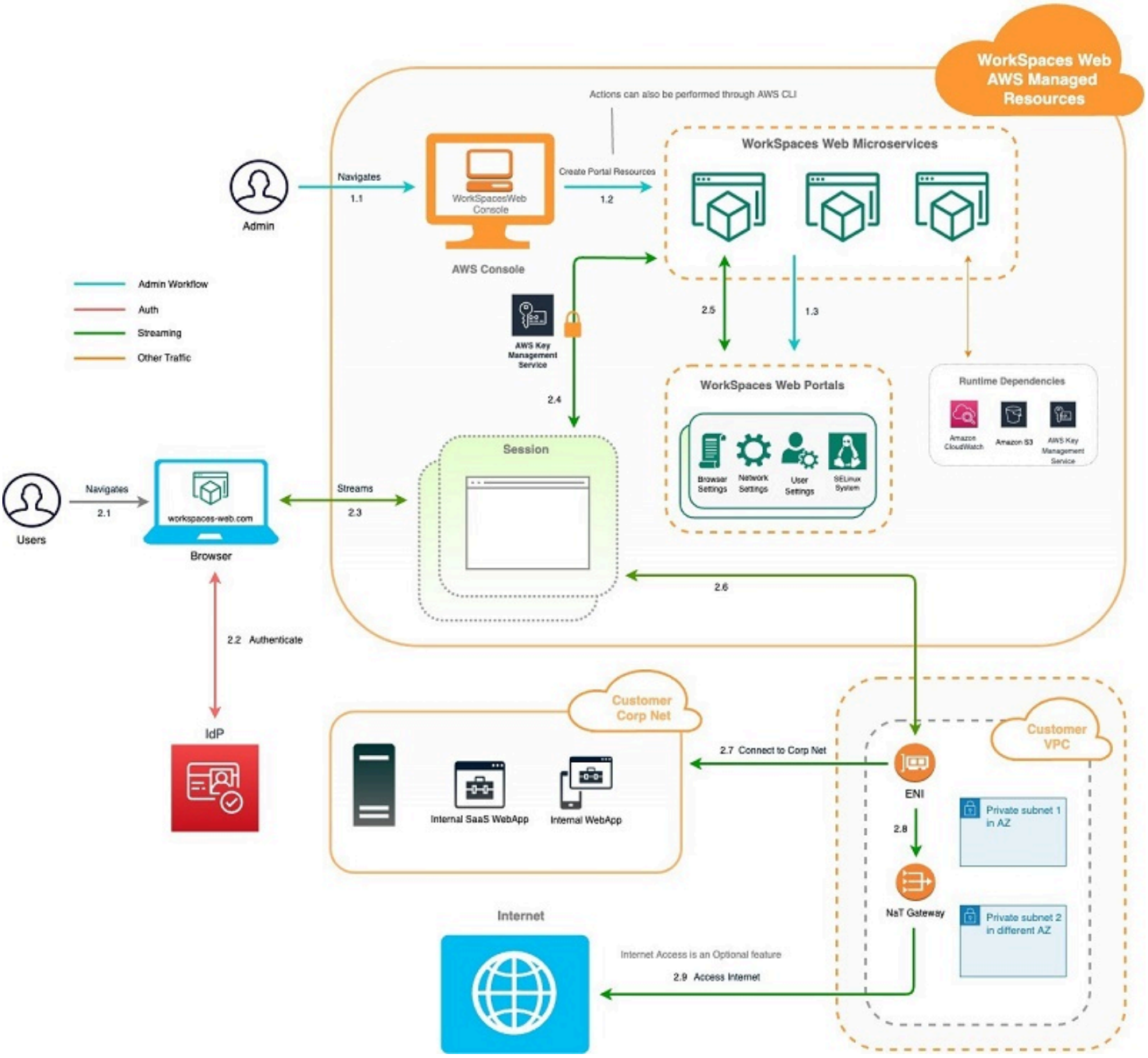
Endpoint tersedia untuk umum di internet dan dapat disematkan ke dalam jaringan Anda.

Layanan terkait

WorkSpaces Web adalah kemampuan dari Amazon WorkSpaces dalam portofolio AWS End User Computing. Dibandingkan dengan WorkSpaces dan AppStream 2.0, WorkSpaces Web dibangun khusus untuk memfasilitasi aman, beban kerja berbasis web. WorkSpaces Web dikelola secara otomatis, dengan kapasitas, penskalaan, dan gambar yang disediakan dan diperbarui sesuai permintaan oleh AWS. Misalnya, Anda dapat memilih untuk menawarkan Workspace Desktop persisten kepada pengembang perangkat lunak Anda yang membutuhkan akses ke sumber daya desktop, dan Amazon WorkSpaces Web kepada 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 Web.



Mengakses Amazon WorkSpaces Web

Administrator mengakses Amazon WorkSpaces Web melalui AWS WorkSpaces Web Console, SDK, CLI, atau API. Pengguna Anda mengaksesnya melalui titik akhir Amazon WorkSpaces Web.

Menyiapkan Amazon WorkSpaces Web

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

Topik

Mendaftar dan membuat pengguna

Mendaftar Akun AWS

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

Untuk mendaftar Akun AWS

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

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

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

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

Membuat pengguna administratif

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

Mengamankan Pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat email Akun AWS Anda. Di halaman berikutnya, masukkan kata sandi Anda.

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

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

Membuat pengguna 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 sebuah pengguna administratif.

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

Masuk sebagai pengguna administratif

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

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

Memberikan akses terprogram

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

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

Pengguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, SDK AWS, atau API AWS.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengonfigurasi AWS CLI untuk menggunakan AWS IAM Identity Center di Panduan Pengguna AWS Command Line Interface. • Untuk SDK AWS, alat, dan API AWS, lihat Autentikasi Pusat Identitas IAM di Panduan Referensi SDK dan Alat AWS.
IAM	Gunakan kredensial sementara untuk menandatangani permintaan terprogram ke AWS CLI, SDK AWS, atau API AWS.	Mengikuti petunjuk dalam Menggunakan kredensial sementara dengan sumber daya AWS di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensial jangka panjang untuk menandatangani permintaan terprogram	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan.

Pengguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
	ke AWS CLI, SDK AWS, atau API AWS.	• Untuk AWS CLI, lihat Mengautentikasi menggunakan kredensial pengguna IAM di Panduan Pengguna AWS Command Line Interface. • Untuk SDK dan alat AWS, lihat Mengautentikasi menggunakan kredensial jangka panjang di Panduan Referensi SDK dan Alat AWS. • Untuk API AWS, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Jaringan dan akses

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

Topik

Persyaratan VPC

Selama pembuatan portal WorkSpaces Web, 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 WorkSpaces Web 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 WorkSpaces Web.

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 Web 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 WorkSpaces Web 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 Anda membuat VPC Anda, Anda harus mengalokasikan alamat IP Elastis di Wilayah Web Anda WorkSpaces . 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 Web 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 Web 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 Web 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 Anda membuat dan mengonfigurasi VPC Anda, 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 Web 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.
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 Web 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 akhir S3) [PL-ID (com.amazonaws.region.s3)]	Penyimpanan (VPCE-ID)	Lalu lintas yang ditujukan untuk bucket S3 dialihkan ke titik akhir S3 (diidentifikasi oleh VPCE-ID).

9. Di panel navigasi, pilih Pengguna. Kemudian pilih subnet pribadi kedua yang Anda buat (misalnya,**`WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web, Anda dapat mengatur pengaturan proxy menggunakan kebijakan Chrome yang ada di browser web. Anda dapat melakukan ini dengan menyiapkan proxy keluar HTTP untuk WorkSpaces Web.

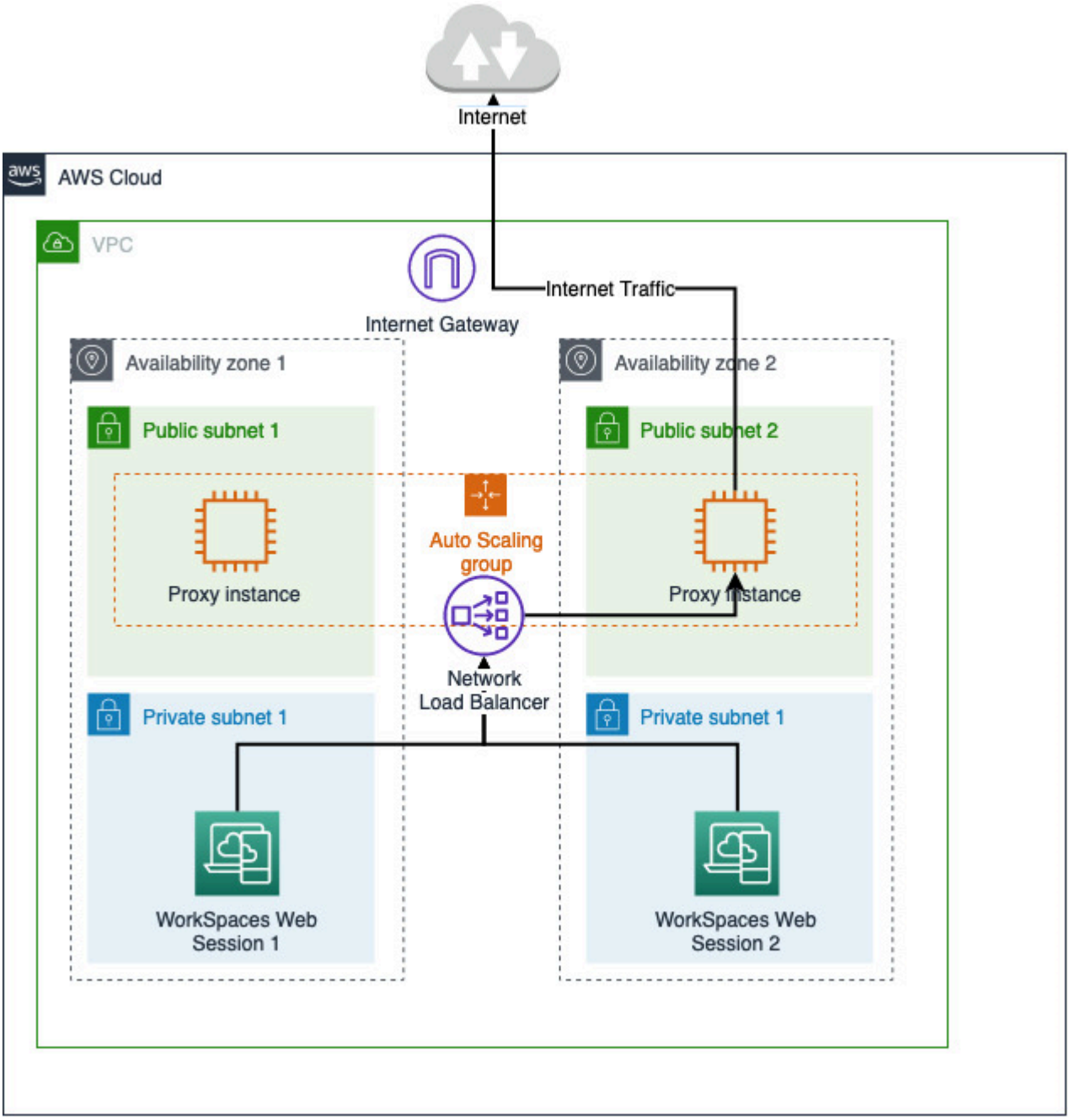
Solusi ini didasarkan pada pengaturan proxy VPC keluar yang direkomendasikan. Solusi proxy didasarkan pada open source HTTP proxy Squid. Kemudian, ia menggunakan pengaturan browser WorkSpaces Web untuk mengkonfigurasi portal WorkSpaces Web untuk terhubung ke titik akhir proxy. Untuk informasi selengkapnya, 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 WorkSpaces Web dikerahkan ke 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 WorkSpaces Web 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 WorkSpaces sesi Web.



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 Anda, lihat VPC default.

- Anda memerlukan satu titik akhir proxy tunggal yang dapat diakses dari subnet pribadi, tempat sesi WorkSpaces Web 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.

Menyiapkan proxy keluar HTTP untuk Web WorkSpaces

Untuk menyiapkan proxy keluar HTTP untuk WorkSpaces Web, 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 penerapan, temukan parameter CloudFormation output OutboundProxyDomaindan 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 WorkSpaces Web, 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 WorkSpaces Web 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 WorkSpaces Web Anda berhasil menelusuri konten internet tanpa gateway NAT. Di CloudWatch Log, verifikasi bahwa log akses proxy Squid direkam.

Memecahkan masalah

Setelah kebijakan Chrome diterapkan, jika sesi WorkSpaces Web 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 WorkSpaces Web Anda tinggal. Untuk melakukan ini, buat instans EC2 di subnet pribadi, dan uji koneksi dari instans EC2 pribadi ke titik akhir proxy Anda.
- Pastikan proxy memiliki akses internet.
- Pastikan kebijakan Chrome sudah benar.
  - Konfirmasikan pemformatan berikut untuk `ProxyServer` bidang kebijakan:`<Proxy DNS name>:<Proxy port>`. Seharusnya tidak ada `http://` atau `https://` di awalan.
  - Di sesi WorkSpaces Web, 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 WorkSpaces Web Anda (juga disebut sebagai batas) cukup untuk mendukung permintaan yang Anda harapkan. Untuk meminta peningkatan kuota, Anda dapat menggunakan konsol Service Quotas di https://console.aws.amazon.com/servicequotas/. Untuk informasi tentang kuota WorkSpaces Web default, lihatthe section called “Minta peningkatan kuota layanan”.

- 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 Web membutuhkan elastic network interface sendiri selama durasi streaming. WorkSpaces Web 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 WorkSpaces Web memerlukan alamat IP klien yang 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 Web 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 WorkSpaces Web 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 virtual private cloud (VPC) untuk digunakan dengan WorkSpaces Web, subnet VPC Anda harus berada di Availability Zone yang berbeda di Wilayah tempat Anda meluncurkan Web. 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. Sebagai contoh, `use1-az2` adalah ID AZ untuk Wilayah `us-east-1` dan memiliki lokasi yang sama di setiap akun AWS.

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 Web 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 ID AZ, lihat Wilayah, Availability Zone, dan Local Zones di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Koneksi VPC

Setiap instance streaming WorkSpaces Web 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 Web dikonfigurasi untuk merutekan koneksi streaming melalui internet publik. Konektivitas internet diperlukan untuk mengautentikasi pengguna dan mengirimkan aset web yang dibutuhkan WorkSpaces Web untuk 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 WorkSpaces Web.

Topik

Alamat IP dan persyaratan port

Untuk mengakses instans WorkSpaces Web, 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.
  - AWSmenerbitkan 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 menggunakanAWS 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 layanan WorkSpaces Web dari browser lokal mereka, Anda harus menambahkan domain dan alamat IP berikut ke daftar izinkan di jaringan tempat pengguna mencoba mengakses layanan tersebut.

{Region} di bawah ini harus diganti dengan nama operasiWilayah AWS. Misalnya, s3. *{region}* .amazonaws.com harus s3.eu-west-1.amazonaws.com jika itu untuk Eropa (Irlandia) (eu-west-1).

Kategori	Domain atau Alamat IP
WorkSpaces Aset Streaming Web	s3. *{wilayah} .amazonaws.com* s3.amazonaws.com appstream2. *{wilayah} .aws.amazon.com*

Kategori	Domain atau Alamat IP
	*.amazonappstream.com *.shortbread.aws.dev
WorkSpaces WebApp Aset Web	*.workspaces-web.com
WorkSpaces Otentikasi Web	*.auth. *{wilayah}* .amazoncognito.com kognito-identitas. *{wilayah} .amazonaws.com* kognito-idp. *{wilayah} .amazonaws.com* *.cloudfront.net
WorkSpaces Metrik dan Pelaporan Web	*.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 WorkSpaces Web dapat menggunakan penyedia itu. Jika Anda menggunakan Pusat Identitas IAM, lihat prasyarat Pusat Identitas IAM untuk informasi lebih lanjut.

Memulai dengan Amazon WorkSpaces Web

Ikuti langkah-langkah ini untuk membuat portal WorkSpaces web Web dan memberi pengguna akses ke situs web internal dan SaaS dari browser mereka 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 Web 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 Amazon WorkSpaces Web

Topik

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 WorkSpaces Web dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih WorkSpaces Web, lalu portal Web, dan kemudian 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 Web.
    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 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”.
3. 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 Web menyertakan 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.

4. 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)”.
5. 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 Mencetak ke perangkat lokal, pilih Diizinkan atau Tidak diizinkan.
5. 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

WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web

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 diprakarsai 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 Sign 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. Ini dapat mencegah data dicegat dalam pernyataan SAMP antara IDP dan Web. 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 Web mereka dengan satu tindakan.
   a. Unduh sertifikat penandatanganan dari WorkSpaces Web 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 “Bimbingan 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 dimulai 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 WorkSpaces Web" 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 WorkSpaces Web" 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 WorkSpaces Web" 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 WorkSpaces Web.
8. Unduh file pertukaran metadata dari IDP Anda. Anda akan mengunggah metadata ini ke WorkSpaces Web pada langkah berikutnya.

Langkah 3: Selesai mengonfigurasi penyedia identitas Anda di Web WorkSpaces

Kembali ke WorkSpaces Webconsole. 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 WorkSpaces Web, 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 Web 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 Web membutuhkan klaim berikut untuk hadir dalam tanggapan 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>
> ```
>
> - `Response`Klaim dengan `InResponseTo` nilai ID permintaan SAMP asli. Contoh:
>
> ```
> <samlp:Response ... InResponseTo="<originalSAMLrequestId>">
> ```
>
> - `SubjectConfirmationData`Klaim 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 Webmemvalidasi parameter permintaan Anda dan pernyataan SAMP. 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>
```

Bimbingan 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 aplikasi SAMP	Manajemen pengguna	Referensi bidang Wizard Integrasi Aplikasi SAMP	Referensi bidang Wizard Integrasi Aplikasi SAMP	Referensi bidang Wizard Integrasi Aplikasi SAMP	Referensi bidang Wizard 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	Apakah PingOne untuk Enterprise mendukung enkripsi?	SAMP 2.0 logout tunggal

IdP	Pengaturan aplikasi SAMP	Manajemen pengguna	Autentikasi yang diprakarsai IDP	Permintaan penandatanganan	Enkripsi pernyataan	Keluar tunggal
				Enterprise PingOne		
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)
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 WorkSpaces Web 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 WorkSpaces Web 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 Anda kaitkan dapat masuk ke WorkSpaces Web 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 WorkSpaces Web dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih WorkSpaces Web, 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 WorkSpaces Web 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 WorkSpaces Webportal. 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 WorkSpaces Web 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 WorkSpaces Web di https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih WorkSpaces Web, 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. Di halaman login WorkSpaces Web, pilih Masuk, SAMP, dan masukkan kredensyal SAMP Anda.

5. Ketika Anda melihat halaman sesi Anda sedang dipersiapkan, sesi WorkSpaces Web 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 WorkSpaces Web, Anda memilih dari opsi berikut untuk mendistribusikan portal:

- Tambahkan portal Anda ke gateway aplikasi SAMP Anda bagi pengguna untuk meluncurkan sesi dari IDP mereka secara langsung. Misalnya, 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 setiap Wilayah AWS tempat WorkSpaces Web tersedia. Setiap portal web dapat mendukung hingga 25 koneksi pengguna setiap saat. Untuk meningkatkan jumlah portal yang dapat Anda buat di Wilayah, atau untuk mendukung lebih banyak sesi bersamaan untuk portal, lihat. the section called “Minta peningkatan kuota layanan”

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

Untuk melihat detail portal web

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

Mengedit portal web

Untuk mengedit portal web

1. Buka konsol WorkSpaces Web dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.

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

Minta peningkatan kuota layanan

Saat Anda membuat AWS akun, kami secara otomatis menetapkan kuota layanan default (juga disebut sebagai batas) untuk penggunaan sumber daya dengan AWS Layanan. WorkSpaces Web menetapkan kuota pada dua jenis sumber daya - portal web (per wilayah) dan sesi bersamaan maksimum (per portal web). WorkSpaces Web saat ini memiliki batas kuota layanan berikut:

Kuota default dalam akun Wilayah AWS menurut	Nilai
Portal web	1
Sesi bersamaan maksimum	25

Portal web adalah sumber daya dasar dalam WorkSpaces Web. Ini adalah hubungan antara penyedia identitas SAMP 2.0 Anda, dan koneksi jaringan Anda ke internet dan konten Anda. Anda

dapat membuat portal web di Wilayah AWS mana pun WorkSpaces Web tersedia. Lihat tabel wilayah untuk ketersediaan saat ini.

Sesi bersamaan maksimum adalah jumlah pengguna tertinggi yang akan terhubung pada saat yang sama ke portal web tertentu. Jika batas kuota layanan untuk sesi bersamaan maksimum tidak ditetapkan dengan tepat, pengguna mungkin menemukan bahwa sesi mereka tidak tersedia saat mereka masuk ke Web. WorkSpaces Anda juga harus memastikan bahwa VPC dan subnet Anda memiliki ruang IP yang cukup untuk mendukung sesi bersamaan maksimum, atau pengguna mungkin tidak dapat terhubung ke sesi.

Misalnya, pelanggan memiliki dua portal web di AS Timur (Virginia N.) dan 125 pengguna. Portal web pertama (portal A) memiliki 25 pengguna dan tidak memerlukan peningkatan kuota layanan. Portal web kedua (portal B) harus tersedia hingga 100 pengguna. Pengguna ini tersebar di dua shift, dan jam kerja mereka tidak tumpang tindih. Oleh karena itu, pelanggan perlu meminta peningkatan kuota layanan untuk Portal B menjadi sesi konkuren maksimum 50 pengguna.

Anda dapat meminta kenaikan untuk salah satu dari batas kuota layanan ini. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota.

Meminta peningkatan kuota layanan

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

> **Important**
>
> WorkSpaces Kuota layanan web mempengaruhi 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.

Kontrol interval untuk mengautentikasi ulang token IDP SAMP

Saat pengguna mengunjungi portal WorkSpaces Web, mereka dapat masuk untuk meluncurkan sesi streaming. Setiap sesi dimulai di halaman awal, kecuali 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 kredensialnya masuk.

Jika pengguna memiliki token SAMP iDP yang valid, mereka dapat WorkSpaces mengakses Web. 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 Web Anda dan nilai batas waktu idle. Nilai-nilai ini mengontrol jumlah waktu antara interaksi terakhir pengguna dan ketika sesi WorkSpaces Web 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 IDP SAMP yang valid, mereka tidak perlu memasukkan nama pengguna dan kata sandi mereka untuk memulai sesi Web 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 WorkSpaces Web.
- Akhir sesi - Menandai akhir sesi WorkSpaces Web.
- 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 WorkSpaces Web mereka, dan memastikan bahwa penggunaan WorkSpaces Web mereka mematuhi semua hukum dan peraturan yang berlaku. Ini termasuk undang-undang yang mengatur kemampuan majikan untuk memantau penggunaan WorkSpaces Web karyawan, termasuk kegiatan yang dilakukan dalam aplikasi.

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

Untuk mengaktifkan pencatatan akses pengguna di konsol WorkSpaces Web, 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 WorkSpaces Web, Anda harus memiliki Amazon Kinesis Data Stream 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 WorkSpaces Web, Anda dapat menetapkan 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 Amazon WorkSpaces Web.

WorkSpaces Web menerapkan konfigurasi kebijakan browser dasar ke semua portal bersama dengan 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 selengkapnya 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

Untuk mengunggah file JSON kebijakan Chrome Anda, Anda harus membuat portal WorkSpaces Web. 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 dipasang.
   - 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 WorkSpaces Web dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih WorkSpaces Web, 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 Web 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 web 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 WorkSpaces Web:

- 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 WorkSpaces Web Anda, hubungi. AWS Support

Konfigurasikan lokalisasi dalam sesi

Ketika pengguna memulai sesi, WorkSpaces Web 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 Web. 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 - China (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 dalam pelokalan dukungan WorkSpaces Web:

- WorkSpaces Halaman masuk web
- WorkSpaces Pesan status portal web (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 Web memungkinkan Anda untuk mengontrol alamat IP mana portal web Anda dapat diakses dari. 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 Web 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 Web terus memantau alamat IP pengguna untuk memastikan mereka tetap terhubung dari jaringan tepercaya. Jika IP pengguna berubah, WorkSpaces Web 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 WorkSpaces Web mereka, dan harus memastikan bahwa penggunaan WorkSpaces Web mereka mematuhi semua hukum dan peraturan yang berlaku. Ini termasuk undang-undang yang mengatur kemampuan pemberi kerja untuk memantau penggunaan WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web 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 setelan 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 WorkSpaces Web 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 dapat menambahkan ekstensi ke browser Chrome mereka dari toko web Chrome, atau ke FireFox browser mereka dari Add-on untuk FireFox.

Ekstensi tidak diaktifkan di Chrome di InCognito windows. Firefox memiliki pengaturan untuk mengizinkan ekstensi selama penjelajahan pribadi. Untuk informasi selengkapnya, 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
Iklan Azure	microsoftonline.com
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 WorkSpaces Web dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
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 WorkSpaces Web dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
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 WorkSpaces Web 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 WorkSpaces Web 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 WorkSpaces Web dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih WorkSpaces Web, 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.

Keamanan di Amazon WorkSpaces Web

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

Keamanan adalah tanggung jawab bersama antara 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 layanan-layanan AWS di dalam AWS Cloud. AWS juga memberikan Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga melakukan pengujian dan verifikasi secara berkala terhadap efektivitas keamanan kami sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari tentang program . WorkSpaces
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku untuk data Anda.

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

Konten

Perlindungan data di Amazon WorkSpaces Web

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon WorkSpaces Web. Sebagaimana diuraikan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk memelihara kendali atas isi yang dihost pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya lindungi kredensial Akun AWS dan siapkan untuk masing-masing pengguna 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 autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya AWS. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pengelogan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama semua kontrol keamanan bawaan dalam 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 modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

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 saat Anda bekerja dengan WorkSpaces Web atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. 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. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data

Amazon WorkSpaces Web mengumpulkan data kustomisasi portal, seperti pengaturan browser, pengaturan pengguna, pengaturan jaringan, informasi penyedia identitas, data penyimpanan kepercayaan, dan data sertifikat toko kepercayaan. WorkSpaces Web juga mengumpulkan data kebijakan browser, preferensi pengguna (untuk pengaturan browser), dan log sesi. Data yang dikumpulkan disimpan di Amazon DynamoDB dan Amazon S3. WorkSpaces Web 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 WorkSpaces Web. Gunakan templat IAM untuk membuat peran Akses Penuh atau peran Hanya Baca. Untuk informasi selengkapnya, lihat AWSkebijakan terkelola untuk WorkSpaces Web.
- Lindungi data dari ujung ke ujung dengan menyediakan kunci yang dikelola pelanggan, sehingga WorkSpaces Web dapat mengenkripsi data Anda saat istirahat dengan kunci yang Anda berikan.
- Hati-hati dengan berbagi domain portal dan kredensyal pengguna:
  - Admin diminta untuk masuk ke WorkSpaces konsol Amazon, dan pengguna diharuskan masuk ke portal WorkSpaces Web.
  - Siapa pun di internet dapat mengakses portal web, tetapi mereka tidak dapat memulai sesi kecuali mereka memiliki kredensyal 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 Web mengamankan konten dan metadata secara default dengan mengenkripsi semua data sensitif dengan. AWS KMS Ini mengumpulkan kebijakan browser dan preferensi pengguna untuk menegakkan kebijakan dan pengaturan selama sesi WorkSpaces Web. 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 WorkSpaces Web dienkripsi menggunakan. AWS KMS WorkSpaces Web 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 WorkSpaces Web. Jika data yang merupakan bagian dari sumber daya tersebut dienkripsi, WorkSpaces Web menerima `customerManagedKeyArn` bidang tersebut sebagai bagian dari API. `create` 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, WorkSpaces Web 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 dalam bergerak

WorkSpaces Web mengenkripsi data dalam perjalanan melalui HTTPS dan TLS 1.2. Anda dapat mengirim permintaan WorkSpaces dengan menggunakan konsol atau panggilan API langsung. Data permintaan yang ditransfer dienkripsi dengan mengirimkan semuanya melalui koneksi HTTPS atau TLS. Data permintaan dapat ditransfer dari AWS KonsolAWS Command Line Interface, atau AWS SDK ke WorkSpaces Web.

Enkripsi dalam perjalanan 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, WorkSpaces Web akan menggunakan Kunci yang AWS Dimiliki. Anda dapat mengatur kunci Anda menggunakan AWS SDK.

Privasi lalu lintas antar jaringan

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

Untuk mengamankan koneksi antar akun, WorkSpaces Web 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 Web WorkSpaces.

Pencatatan akses pengguna

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

Identity and Access Management untuk Amazon WorkSpaces Web

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

Topik

- Mengelola akses menggunakan kebijakan
- Bagaimana Amazon WorkSpaces Web bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Amazon Web WorkSpaces
- AWSkebijakan terkelola untuk WorkSpaces Web
- Memecahkan masalah identitas dan WorkSpaces akses Amazon Web
- Menggunakan peran terkait layanan untuk Web WorkSpaces

Audiens

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

Pengguna layanan — Jika Anda menggunakan layanan WorkSpaces Web untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensyal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur WorkSpaces Web 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 WorkSpaces Web, lihatMemecahkan masalah identitas dan WorkSpaces akses Amazon Web.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya WorkSpaces Web di perusahaan Anda, Anda mungkin memiliki akses penuh ke WorkSpaces Web. Tugas Anda adalah menentukan fitur dan sumber daya WorkSpaces Web mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan WorkSpaces Web, lihatBagaimana Amazon WorkSpaces Web bekerja dengan IAM.

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

Mengautentikasi dengan identitas

Autentikasi adalah cara Anda untuk masuk ke AWS menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. Pengguna AWS IAM Identity Center Pengguna (Pusat Identitas IAM), autentikasi Single Sign-On perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas gabungan, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

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

Jika Anda mengakses AWS secara terprogram, AWS memberikan Kit Pengembangan Perangkat Lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan peralatan AWS, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang cara menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan API AWS dalam Panduan Pengguna IAM.

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

Pengguna root Akun AWS

Ketika membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses penuh ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar tugas lengkap yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Praktik terbaiknya adalah mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial temporer.

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

Untuk pengelolaan akses terpusat, sebaiknya Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa yang dimaksud Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya andalkan kredensial temporer, dan bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, sebaiknya rotasikan kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

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

Peran IAM

Peran IAM merupakan identitas dalam Akun AWS Anda yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara dalam AWS Management Console dengan berganti peran. Anda dapat mengambil peran dengan cara memanggil operasi API AWS CLI atau AWS atau menggunakan URL kustom. Untuk informasi selengkapnya tentang metode untuk menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Saat identitas terfederasi diautentikasi, identitas tersebut dikaitkan dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi sekumpulan izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengaitkan izin yang ditetapkan ke peran dalam IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center.
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat menyertakan kebijakan secara langsung ke sumber daya (bukan menggunakan peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Contoh, ketika Anda melakukan panggilan dalam layanan, umumnya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Saat menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian dilanjutkan

oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya diajukan saat layanan menerima permintaan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Meneruskan sesi akses.

- Peran IAM – Peran layanan adalah peran IAM yang diambil layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran terkait layanan – Peran terkait layanan adalah tipe peran layanan yang terkait dengan Layanan AWS. Layanan tersebut dapat mengambil peran untuk melakukan sebuah tindakan atas nama Anda. Peran terkait layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan peran IAM untuk mengelola kredensial sementara untuk aplikasi yang berjalan di instans EC2 dan mengajukan permintaan API AWS CLI atau AWS. Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan peran AWS ke instans EC2 dan menyediakannya bagi semua aplikasinya, Anda dapat membuat profil instans yang dilampirkan ke instans tersebut. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, pengguna root, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan

isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses terhadap apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau API AWS.

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. 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 di Akun AWS Anda. Kebijakan terkelola meliputi kebijakan yang dikelola AWS dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat Memilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

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

dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

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

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Developer Layanan Penyimpanan Ringkas Amazon.

Tipe kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran 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 secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – SCP adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola beberapa akun Akun AWS yang dimiliki bisnis Anda secara terpusat. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. 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 eksplisit di salah satu kebijakan ini akan membatalkan izin tersebut. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Jika beberapa jenis kebijakan diberlakukan untuk satu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika ada beberapa jenis kebijakan, lihat Logika evaluasi kebijakan dalam Panduan Pengguna IAM.

Bagaimana Amazon WorkSpaces Web bekerja dengan IAM

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

Fitur IAM yang dapat Anda gunakan dengan Amazon Web WorkSpaces

Fitur IAM	WorkSpaces Dukungan web
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci persyaratan kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin pengguna utama	Ya

Fitur IAM	WorkSpaces Dukungan web
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang bagaimana WorkSpaces Web dan AWS layanan lainnya bekerja dengan sebagian besar fitur IAM, lihat AWSlayanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Web WorkSpaces

Mendukung kebijakan berbasis identitas	Ya

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

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta ketentuan terkait jenis tindakan yang diizinkan atau ditolak. Anda tidak dapat menentukan pengguna utama dalam kebijakan berbasis identitas karena kebijakan ini berlaku untuk pengguna atau peran yang dilampiri kebijakan. Untuk mempelajari semua elemen yang dapat digunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Web WorkSpaces

Untuk melihat contoh kebijakan berbasis identitas WorkSpaces Web, lihat. Contoh kebijakan berbasis identitas untuk Amazon Web WorkSpaces

Kebijakan berbasis sumber daya dalam Web WorkSpaces

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

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

Tindakan kebijakan untuk WorkSpaces Web

Mendukung tindakan kebijakan	Ya

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

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

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

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

Tindakan kebijakan di WorkSpaces Web menggunakan awalan berikut sebelum tindakan:

```
workspaces-web
```

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

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

Untuk melihat contoh kebijakan berbasis identitas WorkSpaces Web, lihat. Contoh kebijakan berbasis identitas untuk Amazon Web WorkSpaces

Sumber daya kebijakan untuk WorkSpaces Web

Mendukung sumber daya kebijakan	Ya

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

Elemen kebijakan JSON `Resource` menentukan objek atau beberapa objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, 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 mengindikasikan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

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

Untuk melihat contoh kebijakan berbasis identitas WorkSpaces Web, lihat. Contoh kebijakan berbasis identitas untuk Amazon Web WorkSpaces

Kunci kondisi kebijakan untuk WorkSpaces Web

Mendukung kunci kondisi kebijakan spesifik layanan	Ya

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

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional 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 satu pernyataan, atau beberapa kunci dalam satu elemen `Condition`, AWS akan mengevaluasinya dengan menggunakan operasi `AND` logis. Jika Anda menentukan beberapa niilai untuk satu kunci persyaratan, AWS akan mengevaluasi syarat tersebut menggunakan operasi `OR` yang logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tanda di Panduan Pengguna IAM.

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

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

Untuk melihat contoh kebijakan berbasis identitas WorkSpaces Web, lihat. Contoh kebijakan berbasis identitas untuk Amazon Web WorkSpaces

Daftar kontrol akses (ACL) di Web WorkSpaces

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengontrol pengguna utama (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut (ABAC) dengan Web WorkSpaces

Mendukung ABAC (tanda dalam kebijakan)	Parsial

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Di AWS, atribut ini disebut tag. Anda dapat melampirkan tanda ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS. Pemberian tanda ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-operasi ketika tanda milik pengguna utama cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna dalam situasi di mana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tanda di elemen syarat dari sebuh kebijakan dengan menggunakan kunci-kunci persyaratan `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 hanya untuk beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial terkait langkah-langkah penyiapan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Menggunakan kredensyal Sementara dengan Web WorkSpaces

Mendukung kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensial sementara. Sebagai informasi tambahan, termasuk tentang Layanan AWS mana saja yang berfungsi dengan kredensial sementara, lihat Layanan AWS yang berfungsi dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensial sementara jika Anda masuk ke AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS dengan menggunakan tautan masuk tunggal (SSO) milik perusahaan Anda, proses itu secara otomatis akan membuat kredensial temporer. Anda juga akan membuat kredensial sementara secara otomatis saat masuk ke konsol sebagai pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang cara beralih peran, lihat Beralih peran (konsol) di Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan AWS CLI atau AWS API. Anda kemudian dapat menggunakan kredensial sementara untuk mengakses AWS. AWS menyarankan Anda membuat kredensial sementara secara dinamis, alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Web WorkSpaces

Mendukung sesi akses maju (FAS)	Ya

Jika menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan di AWS, Anda akan dianggap sebagai pengguna utama. Jika menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian dilanjutkan oleh tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya diajukan saat layanan menerima permintaan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua

tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Meneruskan sesi akses.

Peran layanan untuk WorkSpaces Web

Mendukung peran layanan	Tidak

Peran layanan adalah sebuah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas WorkSpaces Web. Edit peran layanan hanya ketika WorkSpaces Web memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Web WorkSpaces

Mendukung peran yang terkait layanan	Ya

Peran yang terkait layanan adalah jenis peran layanan yang terkait dengan Layanan AWS. Layanan ini dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau pengelolaan peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Temukan sebuah 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 Web WorkSpaces

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya WorkSpaces Web. Pengguan dan peran tersebut juga tidak dapat melakukan tugas dengan

menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau API AWS. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

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

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

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol WorkSpaces Web
- Izinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

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

- Mulai menggunakan kebijakan yang dikelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan yang dikelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan ini ada di Akun AWS Anda. Sebaiknya Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Wajibkan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

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

Menggunakan konsol WorkSpaces Web

Untuk mengakses konsol WorkSpaces Web Amazon, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk daftar dan melihat rincian tentang sumber daya WorkSpaces Web di AndaAkun 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 memberikan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau API AWS. Sebaliknya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang coba dilakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol WorkSpaces Web, lampirkan juga kebijakan WorkSpaces Web `ConsoleAccess` atau `ReadOnly` AWS terkelola

ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna di Panduan Pengguna IAM.

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan pada konsol atau menggunakan AWS CLI atau AWS API secara terprogram.

```
{
    "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": "*"
        }
    ]
}
```

AWSkebijakan terkelola untuk WorkSpaces Web

Untuk menambahkan izin ke para pengguna, grup, dan peran, akan lebih mudah menggunakan kebijakan terkelola AWS dibandingkan dengan menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan terkelola pelanggan IAM yang hanya menyediakan izin sesuai kebutuhan tim Anda. Untuk mulai dengan cepat, Anda dapat menggunakan kebijakan-kebijakan terkelola AWS kami. Kebijakan-kebijakan ini mencakup kasus penggunaan umum dan tersedia di akun AWS Anda. Untuk informasi lebih lanjut tentang kebijakan-kebijakan terkelola AWS, lihat kebijakan terkelola AWS di Panduan Pengguna IAM.

Layanan AWS mempertahankan dan memperbarui kebijakan-kebijakan terkelola AWS. Anda tidak dapat mengubah izin yang ada dalam kebijakan-kebijakan yang dikelola AWS. 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-kebijakan terkelola untuk fungsi tugas 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 menambahkan izin hanya-baca untuk operasi dan sumber daya yang baru. Untuk melihat daftar dan deskripsi dari kebijakan-kebijakan fungsi tugas, lihat kebijakan terkelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWSkebijakan terkelola: AmazonWorkSpacesWebServiceRole Kebijakan

Anda tidak dapat melampirkan `AmazonWorkSpacesWebServiceRolePolicy` kebijakan ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan WorkSpaces

Web melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat the section called "Menggunakan Peran Tertaut Layanan".

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

Rincian perizinan

Kebijakan ini mencakup izin berikut:

- `WorkSpaces Web`— Memungkinkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh Amazon WorkSpaces Web.
- `ec2`- Memungkinkan prinsipal untuk menggambarkan VPC, subnet, dan zona ketersediaan; membuat, menandai, menjelaskan, dan menghapus antarmuka jaringan; mengasosiasikan atau memisahkan alamat; dan menjelaskan tabel rute, grup keamanan, dan titik akhir VPC.
- `CloudWatch`- Memungkinkan prinsipal untuk menempatkan data metrik.
- `Kinesis`- Memungkinkan prinsipal untuk menggambarkan 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-*"
        }
    ]
}
```

Kebijakan terkelola AWS: AmazonWorkSpacesWebReadOnly

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

Kebijakan ini memberikan izin baca-saja yang memungkinkan akses ke WorkSpaces Web dan dependensi melalui AWS ManagementConsole, 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`.

Rincian perizinan

Kebijakan ini mencakup izin berikut.

- `WorkSpaces Web`— Menyediakan akses hanya-baca ke Amazon WorkSpaces Web dan dependensinya melalui AWS Management Console, SDK, dan CLI.
- `ec2`- Memungkinkan prinsipal untuk menggambarkan VPC, subnet, dan grup keamanan. Ini digunakan di AWS Management Console di WorkSpaces Web untuk menunjukkan kepada Anda VPC, subnet, dan grup keamanan yang tersedia untuk digunakan dengan layanan ini.
- `Kinesis`- Memungkinkan prinsipal untuk mencantumkan aliran data Kinesis. Ini digunakan di AWS Management Console di WorkSpaces Web untuk menampilkan 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": "*"
        }
    ]
}
```

WorkSpacesPembaruan web untuk kebijakan AWS terkelola

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

Perubahan	Deskripsi	Tanggal
AmazonWorkSpacesWebServiceRolePolicy- Kebijakan yang diperbarui	WorkSpacesWeb memperbarui kebijakan CreateNetworkInterface untuk membatasi tag dengan aws:RequestTag/WorkSpacesWebManaged: true dan bertindak pada sumber daya subnet dan grup keamanan, serta membatasi DeleteNetworkInterface	15 Desember 15 Desember 15 Desember 15 Desember 15 Desember 15 Desember 15 Desember 15

Perubahan	Deskripsi	Tanggal
	ENI yang ditandai dengan aws:/: ResourceTag true. WorkSpacesWebManaged	
AmazonWorkSpacesWebReadOnly- Kebijakan yang diperbarui	WorkSpacesWeb 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 2 November 2 November 2 November 2 November 2 November 2 November 2 November 2
AmazonWorkSpacesWebServiceRolePolicy- Kebijakan yang diperbarui	WorkSpacesWeb 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”.	17 Oktober 17 Oktober 17 Oktober 17 Oktober 17 Oktober 17 Oktober 17 Oktober 17 Oktober 17
AmazonWorkSpacesWebServiceRolePolicy- Kebijakan yang diperbarui	WorkSpacesWeb memperbarui kebijakan untuk membuat tag selama pembuatan ENI.	6 September 6 September 6 September 6 September 6 September 6 September 6 September 6 September 6
AmazonWorkSpacesWebServiceRolePolicy- Kebijakan yang diperbarui	WorkSpacesWeb memperbarui kebijakan untuk menambahkan namespace AWS/Usage ke izin API. PutMetricData	6 April 6 April 6 Juli 6 April 6 April 6 April 6

Perubahan	Deskripsi	Tanggal
AmazonWorkSpacesWebReadOnly – Kebijakan baru	WorkSpacesWeb menambahkan kebijakan baru untuk menyediakan akses hanya-baca ke Amazon WorkSpaces Web dan dependensinya melalui AWS Management Console, SDK, dan CLI.	30 November 30 November 30 November 30 November 30 November 30
AmazonWorkSpacesWebServiceRolePolicy – Kebijakan baru	WorkSpacesWeb menambahkan kebijakan baru untuk memungkinkan akses ke layanan dan sumber daya AWS yang digunakan atau dikelola oleh Amazon WorkSpaces Web.	30 November 30 November 30 November 30 November 30 November 30
WorkSpacesWeb mulai melacak perubahan	WorkSpacesWeb mulai melacak perubahan untuk kebijakan AWS terkelola.	30 November 30 November 30 November 30 November 30 November 30

Memecahkan masalah identitas dan WorkSpaces akses Amazon Web

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan WorkSpaces Web dan IAM.

Topik

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

Saya tidak berwenang untuk melakukan tindakan di WorkSpaces Web

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

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

```
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 membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

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

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait-layanan. Untuk melakukan tindakan tersebut, Anda harus memiliki izin untuk memberikan peran pada layanan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di WorkSpaces Web. 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 membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

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

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna 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 (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah WorkSpaces Web mendukung fitur-fitur ini, lihatBagaimana Amazon WorkSpaces Web bekerja dengan IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di Akun AWS lainnya yang Anda miliki dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk Web WorkSpaces

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

Peran terkait layanan membuat pengaturan WorkSpaces Web lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. WorkSpacesWeb mendefinisikan izin peran terkait layanannya, dan kecuali ditentukan lain, hanya WorkSpaces Web 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 WorkSpaces Web Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran tertaut layanan, lihat Layanan yang Bekerja dengan IAM AWS dan mencari layanan yang memiliki opsi Ya di kolom Peran Tertaut Layanan. Pilih Yes (Ya) bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Web WorkSpaces

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

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

- `workspaces-web.amazonaws.com`

Kebijakan izin peran bernama `AmazonWorkSpacesWebServiceRolePolicy` memungkinkan WorkSpaces Web 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`
- Aksi: `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 lebih lanjut, lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Web WorkSpaces

Anda tidak perlu membuat peran terkait layanan secara manual. Ketika Anda membuat portal pertama Anda diAWS Management Console,AWS CLI, atau AWS API, WorkSpaces Web menciptakan 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. Ketika Anda membuat portal pertama Anda, WorkSpaces Web menciptakan peran terkait layanan untuk Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan WorkSpacesWeb. Di AWS CLI atau API AWS, buat peran yang terhubung dengan

layanan dengan nama layanan `workspaces-web.amazonaws.com`. 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 Web WorkSpaces

WorkSpacesWeb tidak mengizinkan Anda untuk 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 lebih lanjut, lihat Mengedit Peran Tertaut Layanan di Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Web 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 WorkSpaces Web menggunakan peran ketika Anda mencoba untuk menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya WorkSpaces Web 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, toko kepercayaan, dan pengaturan pencatatan akses pengguna) dari portal Anda, hapus sumber daya ini, lalu hapus portal.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan AWSServiceRoleForAmazonWorkSpacesWeb. Untuk informasi lebih lanjut, lihat Menghapus Peran Tertaut Layanan di Panduan Pengguna IAM.

Wilayah yang didukung untuk WorkSpaces peran terkait layanan Web

WorkSpacesWeb 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 Web

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

Validasi kepatuhan untuk Amazon Web WorkSpaces

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan khusus, lihat Layanan AWS di Scope oleh Program Program Kepatuhan yang Anda minati. Untuk informasi umum, lihat Program Kepatuhan 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 berdasarkan sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Mulai Cepat Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah-langkah untuk melakukan deployment lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.
- Merancang Keamanan dan Kepatuhan HIPAA di Amazon Web Services – Laporan resmi ini menjelaskan cara perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

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

- Sumber Daya Kepatuhan AWS – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Panduan Kepatuhan Pelanggan AWS – Pahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan kontrol keamanan di banyak kerangka kerja (termasuk National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), dan International Organization for Standardization (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan Developer AWS Config – Layanan AWS Config menilai seberapa baik konfigurasi sumber daya Anda dalam mematuhi praktik-praktik internal, pedoman industri, dan regulasi internal.
- AWS Security Hub – Layanan AWS ini memberikan pandangan komprehensif tentang status keamanan Anda di dalam AWS. Security Hub menggunakan kontrol keamanan untuk mengevaluasi sumber daya AWS Anda dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- AWS Audit Manager – Layanan AWS ini akan membantu Anda untuk terus-menerus mengaudit penggunaan AWS untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap regulasi dan standar industri.

Ketahanan di Amazon WorkSpaces Web

Infrastruktur global AWS dibangun di sekitar Wilayah AWS dan Availability Zone. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi yang terhubung dengan jaringan latensi rendah, throughput tinggi, dan jaringan yang sangat berlebihan. Dengan Availability Zone, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis mengalami fail over antar zona tanpa gangguan. Availability Zone memiliki ketersediaan yang lebih baik, toleran terhadap kegagalan, dan dapat diukur skalanya jika dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

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

Berikut ini saat ini tidak didukung oleh WorkSpaces Web:

- Mencadangkan konten di seluruh AZ atau wilayah
- Cadangan terenkripsi
- Mengenkripsi konten dalam transit antara AZ atau wilayah
- backup 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 Web

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

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

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

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

WorkSpacesWeb mengisolasi lalu lintas layanan dengan menerapkan Otentikasi dan Otorisasi AWS SiGv4 Standar ke semua layanan. Titik akhir sumber daya pelanggan (atau endpoint 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 VPC, subnet, atau grup keamanan. Titik akhir multi-tenancy dan VPC (PrivateLink) saat ini tidak didukung.

Analisis konfigurasi dan kelemahan di Amazon WorkSpaces Web

WorkSpaces Web update dan patch aplikasi dan platform yang diperlukan atas nama Anda, termasuk Chrome dan Linux. Anda tidak diharuskan untuk menambal atau membangun kembali. Namun, itu adalah tanggung jawab Anda untuk mengkonfigurasi WorkSpaces Web sesuai dengan spesifikasi dan pedoman, dan untuk memantau penggunaan WorkSpaces Web oleh pengguna Anda. Semua konfigurasi terkait layanan dan analisis kerentanan adalah tanggung jawab WorkSpaces Web.

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

Praktik terbaik keamanan WorkSpaces untuk

Amazon WorkSpaces Web menyediakan sejumlah fitur keamanan untuk Anda 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 cukup untuk lingkungan Anda, anggap praktik terbaik tersebut sebagai pertimbangan yang membantu dan bukan sebagai rekomendasi.

Praktik terbaik untuk Amazon WorkSpaces Web mencakup hal-hal berikut:

- Untuk mendeteksi potensi peristiwa keamanan yang terkait dengan penggunaan WorkSpaces Web, penggunaan,AWS CloudTrail atau Amazon CloudWatch untuk mendeteksi dan melacak riwayat akses dan log proses. Untuk informasi selengkapnya, lihat Memantau WorkSpaces Web Amazon dengan Amazon CloudWatch dan Membuat log panggilan Amazon WorkSpaces Web API menggunakanAWS CloudTrail.
- Untuk menerapkan kontrol detektif dan mengidentifikasi anomali, gunakan CloudTrail log dan CloudWatch metrik. Untuk informasi selengkapnya, lihat Memantau WorkSpaces Web Amazon dengan Amazon CloudWatch dan Membuat log panggilan Amazon WorkSpaces Web API menggunakanAWS 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 WorkSpaces Web Anda, ikuti praktik terbaik berikut:

- Menerapkan akses hak istimewa setidaknya dan membuat peran tertentu yang akan digunakan untuk tindakan WorkSpaces Web. Gunakan template IAM untuk membuat peran Akses Penuh atau Hanya Baca. Untuk informasi selengkapnya, lihat AWSkebijakan terkelola untuk WorkSpaces Web.
- 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.

Pemantauan Amazon WorkSpaces Web

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon WorkSpaces Web dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk mengawasi portal WorkSpaces Web 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 tahan lama. 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 WorkSpaces Web Amazon dengan Amazon CloudWatch

Anda dapat memantau Amazon WorkSpaces Web menggunakan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. 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 Web WorkSpaces

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

Metrik	Deskripsi	Dimensi	Statistik	Unit
`GlobalMemoryPercent`	Penggunaan memori (RAM) dari instans sesi Amazon WorkSpaces Web.	`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.

Membuat log panggilan Amazon WorkSpaces Web API menggunakanAWS CloudTrail

Amazon WorkSpaces Web terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang dilakukan oleh pengguna, peran, atauAWS layanan di Amazon WorkSpaces Web. CloudTrail menangkap semua panggilan API untuk Amazon WorkSpaces Web sebagai peristiwa. Ini mencakup panggilan dari konsol Amazon WorkSpaces Web dan panggilan kode ke operasi API Amazon WorkSpaces Web. Jika membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa berkelanjutan ke bucket Amazon S3, termasuk peristiwa untuk Amazon WorkSpaces Web. Jika Anda tidak dapat mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol di Riwayat peristiwa. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat mengidentifikasi permintaan yang dibuat ke Amazon WorkSpaces Web, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan dibuat, serta detail lainnya.

Untuk mempelajari lebih lanjut CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

Informasi Amazon WorkSpaces Web di CloudTrail

CloudTrail diaktifkan diAWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Amazon WorkSpaces Web, aktivitas tersebut dicatat dalam CloudTrail peristiwa bersama peristiwaAWS

layanan lainnya di Riwayat peristiwa. Di Riwayat peristiwa, Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru diAWS akun Anda. Untuk informasi lebih lanjut, lihat Melihat peristiwa dengan riwayat CloudTrail peristiwa.

Untuk catatan peristiwa yang sedang berlangsung diAWS akun Anda, termasuk peristiwa untuk Amazon WorkSpaces Web, Anda dapat membuat jejak. Jejak memungkinkan CloudTrail untuk mengirim berkas log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasiAWS layanan lainnya untuk dianalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail Layanan yang didukung dan integrasi
- Mengkonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima Berkas CloudTrail Log dari Beberapa Wilayah dan Menerima Berkas CloudTrail Log dari Beberapa Akun

Semua tindakan Amazon WorkSpaces Web 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:

- Jika permintaan tersebut dibuat dengan kredensial pengguna root atau IAM.
- Jika permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna federasi.
- Bahwa permintaan dibuat oleh layanan AWS lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log Amazon WorkSpaces Web

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang telah Anda tentukan. CloudTrail Berkas log berisi satu atau beberapa entri log. Sebuah peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan detail lainnya. CloudTrail Berkas log bukan merupakan jejak tumpukan terurut dari panggilan API publik, sehingga berkas 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 Web 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. Lihat informasi yang lebih lengkap di the section called “Siapkan pencatatan akses pengguna”.

Panduan untuk pengguna WorkSpaces Web Amazon

Administrator menggunakan Amazon WorkSpaces Web 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 WorkSpaces Web Amazon, meluncurkan dan mengonfigurasi sesi, serta menggunakan bilah alat dan browser web.

Topik

Kompatibilitas browser dan perangkat

Amazon WorkSpaces Web 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).

Panduan sesi

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

Topik

Mulai sesi

Setelah Anda masuk untuk meluncurkan sesi, Anda akan melihat pesan sesi peluncuran dan bilah kemajuan. Ini menunjukkan bahwa Amazon WorkSpaces Web membuat sesi untuk Anda. Di belakang layar, Amazon WorkSpaces Web 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 Web 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 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 Web 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.

Memecahkan masalah

Portal WorkSpaces Web 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 Web 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 Web 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 Web membangun 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 dikirimkan 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 dari toko web browser 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 pada tab penjelajahan normal, alih-alih Incognito (Chrome) atau penjelajahan pribadi (Firefox).

Memecahkan masalah

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

1. Pastikan Anda memiliki ekstensi WorkSpaces Web Amazon yang 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 penjelajahan pribadi (Firefox). Mode ini dapat menyebabkan masalah dengan ekstensi.
3. Jika masalah berlanjut, hubungi administrator portal Anda untuk bantuan tambahan.

Riwayat dokumen untuk Panduan Pengguna WorkSpaces Web Amazon

Tabel berikut menjelaskan rilis dokumentasi untuk Amazon WorkSpaces Web.

Perubahan	Deskripsi	Tanggal
CloudWatch metrik	Ditambahkan GlobalCpu Percent dan GlobalMem oryPercent 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 Web	Menambahkan konten untuk membantu memandu pengguna akhir, yang ingin mempelajari lebih lanjut tentang mengakses WorkSpaces Web Amazon, meluncurkan dan mengonfig urasi sesi, serta menggunakan bilah alat dan browser web.	Juli 17, 2023

Kontrol akses IP	WorkSpaces Web memungkinkan Anda untuk mengontrol alamat IP mana portal web Anda dapat diakses dari.	31 Mei 2023
Pembaruan kebijakan terkelola	Kebijakan AmazonWorkSpacesWebReadOnly terkelola yang diperbarui	15 Mei 2023
Konfigurasikan pembaruan penyedia identitas	WorkSpaces Web menawarkan dua jenis otentikasi: Standar dan AWS IAM Identity Center	15 Maret 2023
Pembaruan kebijakan browser	Bagian kebijakan browser yang diperbarui dan direstrukturisasi	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 WorkSpaces Web	30 November 2021

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