aws

Panduan Administrator

Klien WorkSpaces Tipis Amazon

Klien WorkSpaces Tipis Amazon: Panduan Administrator

Table of Contents

Apa itu konsol administrator Amazon WorkSpaces Thin Client?

Dengan konsol administrator Amazon WorkSpaces Thin Client, administrator dapat mengelola lingkungan dan perangkat WorkSpaces Thin Client melalui portal WorkSpaces Thin Client. Dari konsol web ini, administrator dapat membuat lingkungan, mengelola perangkat, dan mengatur parameter untuk pengguna WorkSpaces Thin Client dalam jaringan mereka.

Lingkungan desktop virtual yang Anda gunakan untuk WorkSpaces Thin Client harus dibuat atau dimodifikasi dalam konsol mereka sendiri.

> **Important**
>
> Agar konsol administrator WorkSpaces Thin Client berfungsi dengan baik, sistem Anda harus terlebih dahulu memenuhi persyaratan tertentu. Persyaratan ini tercantum dalam Prasyarat dan Konfigurasi.

Topik

Apakah Anda pengguna baru?

Jika Anda adalah pengguna pertama kali konsol administrator WorkSpaces Thin Client, kami sarankan Anda mulai dengan membaca bagian berikut:

- Memulai konsol administrator Klien WorkSpaces Tipis
- Menggunakan konsol administrator WorkSpaces Thin Client

Arsitektur

Setiap Klien WorkSpaces Tipis dikaitkan dengan penyedia antarmuka desktop virtual (VDI). WorkSpaces Thin Client mendukung tiga penyedia VDI:

- Amazon WorkSpaces
- AppStream 2.0
- Browser WorkSpaces Aman Amazon

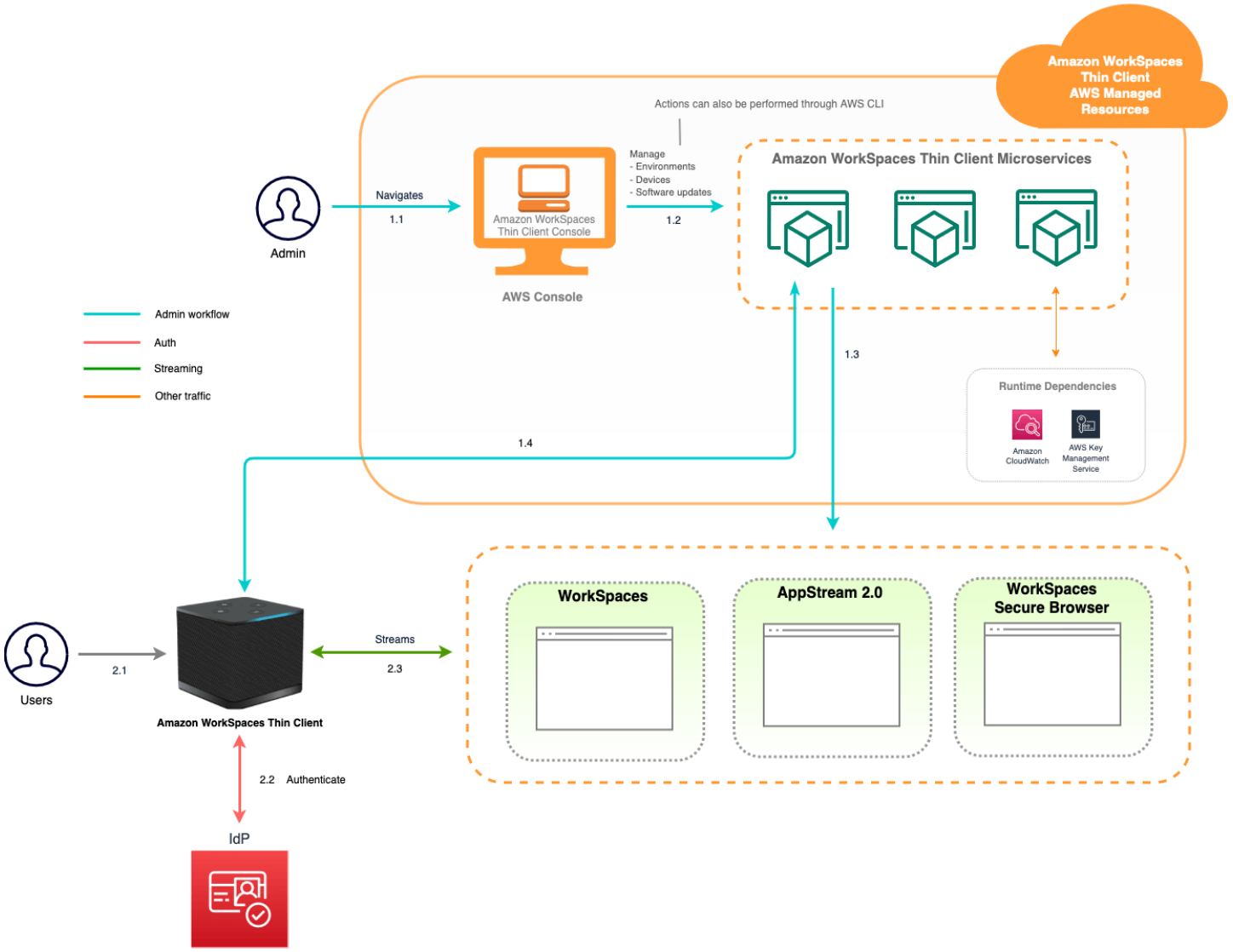
Bergantung pada VDI yang digunakan, informasi untuk Klien WorkSpaces Tipis Anda diakses dan dikelola baik melalui direktori untuk WorkSpaces, tumpukan untuk AppStream 2.0, dan titik akhir portal web untuk Browser Aman. WorkSpaces

Untuk informasi selengkapnya tentang Amazon WorkSpaces, lihat Memulai penyiapan WorkSpaces cepat. Direktori dikelola melalui AWS Directory Service, yang menawarkan opsi berikut: Simple AD, AD Connector, atau AWS Directory Service untuk Microsoft Active Directory, juga dikenal sebagai AWS Managed Microsoft AD. Untuk informasi selengkapnya, lihat Panduan Administrasi AWS Directory Service.

Untuk informasi selengkapnya tentang AppStream 2.0, lihat Memulai Amazon AppStream 2.0: Mengatur Dengan Contoh Aplikasi. AppStream 2.0 mengelola AWS sumber daya yang diperlukan untuk meng-host dan menjalankan aplikasi Anda, menskalakan secara otomatis, dan menyediakan akses ke pengguna sesuai permintaan. AppStream 2.0 memberi pengguna akses ke aplikasi yang mereka butuhkan pada perangkat pilihan mereka, dengan pengalaman pengguna yang responsif dan lancar yang tidak dapat dibedakan dari aplikasi yang diinstal secara asli.

Untuk informasi tentang Browser WorkSpaces Aman, lihat Memulai dengan Amazon WorkSpaces Secure Browser. Amazon WorkSpaces Secure Browser adalah layanan berbasis Linux sesuai 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).

Diagram berikut menunjukkan arsitektur WorkSpaces Thin Client.


Amazon WorkSpaces Thin Client AWS Managed Resources
Actions can also be performed through AWS CLI
Admin
Navigates
1.1
Amazon WorkSpaces Thin Client Console
Manage
- Environments
- Devices
- Software updates
1.2
Amazon WorkSpaces Thin Client Microservices
AWS Console
Admin workflow
Auth
Streaming
Other traffic
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
1.4
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
2.2 Authenticate
IdP

Menyiapkan konsol administrator Amazon WorkSpaces Thin Client

Topik

Daftar AWS

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

Untuk mendaftar untuk Akun AWS

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

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

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

Mmebuat pengguna IAM

Untuk membuat pengguna administrator, pilih salah satu opsi berikut.

Pilih salah satu cara untuk mengelola administrator Anda	Untuk	Oleh	Anda juga bisa
Di Pusat Identitas IAM (Direkomendasikan)	Gunakan kredensi jangka pendek untuk mengakses. AWS Ini sejalan dengan praktik terbaik keamanan. Untuk informasi tentang praktik terbaik, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.	Mengikuti petunjuk di Memulai di Panduan AWS IAM Identity Center Pengguna.	Konfigurasikan akses terprogram dengan Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center dalam AWS Command Line Interface Panduan Pengguna.
Di IAM (Tidak direkomendasikan)	Gunakan kredensi jangka panjang untuk mengakses. AWS	Mengikuti petunjuk dalam Membuat pengguna admin IAM pertama Anda dan grup pengguna di Panduan Pengguna IAM.	Konfigurasikan akses terprogram dengan Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Memulai dengan VDI Anda untuk Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client adalah perangkat thin client hemat biaya yang dibuat untuk bekerja dengan layanan AWS End User Computing untuk memberi Anda akses instan yang aman ke aplikasi dan desktop virtual.

Pilih infrastruktur desktop virtual (VDI), dan konfigurasikan untuk bekerja dengan WorkSpaces Thin Client.

> **Important**
>
> Agar konsol administrator WorkSpaces Thin Client berfungsi dengan baik, sistem Anda harus terlebih dahulu memenuhi persyaratan tertentu. Persyaratan ini tercantum dalam prosedur konfigurasi untuk setiap penyedia desktop virtual.

WorkSpaces Thin Client memerlukan konfigurasi perangkat lunak tertentu, tergantung pada penyedia desktop virtual Anda.

Topik

Mengkonfigurasi WorkSpaces untuk Amazon WorkSpaces Thin Client

Agar WorkSpaces Thin Client dapat digunakan dengan Amazon WorkSpaces, layanan Anda perlu dikonfigurasi untuk mengakses WorkSpaces direktori. Amazon WorkSpaces terdaftar berdasarkan nama direktori mereka di halaman lingkungan WorkSpaces Thin Client Create dalam AWS konsol.

> **Note**
>
> Konfigurasi harus dilakukan sebelum menggunakan konsol untuk pertama kalinya. Anda tidak disarankan memodifikasi fitur prasyarat apa pun setelah Anda mulai menggunakan konsol.

Sebelum Anda mulai

Pastikan Anda memiliki AWS akun untuk membuat atau mengelola. WorkSpace Namun, pengguna perangkat tidak memerlukan AWS akun untuk terhubung dan menggunakannya WorkSpaces.

Tinjau dan pahami konsep-konsep berikut sebelum Anda melanjutkan konfigurasi Anda:

- Saat Anda meluncurkan WorkSpace, pilih WorkSpace bundel. Untuk informasi selengkapnya, lihat Amazon WorkSpaces Bundles.
- Saat Anda meluncurkan WorkSpace, pilih protokol mana yang ingin Anda gunakan dengan bundel Anda. Untuk informasi selengkapnya, lihat Protokol untuk Amazon. WorkSpaces
- Saat Anda meluncurkan WorkSpace, tentukan informasi profil untuk setiap pengguna, termasuk nama pengguna dan alamat email. Pengguna melengkapi profil mereka dengan membuat kata sandi. Informasi tentang WorkSpaces dan pengguna disimpan dalam direktori. Untuk informasi selengkapnya, lihat Mengelola direktori untuk WorkSpaces.
- Saat Anda meluncurkan WorkSpace, mengaktifkan dan mengkonfigurasi akses WorkSpaces web. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasi Akses WorkSpaces Web Amazon

Langkah 1: Verifikasi bahwa sistem Anda memenuhi fitur WorkSpaces yang diperlukan

Agar konsol administrator WorkSpaces Thin Client berfungsi dengan baik dengan Amazon WorkSpaces, sistem Anda harus memenuhi persyaratan spesifik berikut. Tabel ini mencantumkan semua fitur yang didukung ini dan persyaratannya.

Fitur	Persyaratan
Akses web	Diaktifkan
Sistem operasi yang didukung	• Windows 10

Fitur	Persyaratan
	• Windows 10 (Bawa Lisensi Anda Sendiri) • Windows 11 • Windows 11 (Bawa Lisensi Anda Sendiri)
Bundel yang didukung	• Microsoft Power dengan Windows 10 (berbasis Server 2016, 2019, dan 2022) • Microsoft Power dengan Windows 10 (Server 2016, 2019, dan 2022 berbasis) w Office • Microsoft PowerPro dengan Windows 10 (berbasis Server 2016, 2019, dan 2022) • Microsoft PowerPro dengan Windows 10 (Server 2016, 2019, dan 2022 berbasis) w Office • Kinerja Microsoft dengan Windows 10 (berbasis Server 2016, 2019, dan 2022) • Kinerja Microsoft dengan Windows 10 (Server 2016, 2019, dan 2022 berbasis) w Office
Protokol yang didukung	Hanya WSP

Langkah 2: Gunakan pengaturan lanjutan untuk meluncurkan WorkSpace

Untuk menggunakan pengaturan lanjutan untuk meluncurkan WorkSpace

1. Buka WorkSpaces konsol dihttps://console.aws.amazon.com/workspaces/.
2. Pilih salah satu jenis direktori berikut, lalu pilih Berikutnya:
   - AWS Dikelola Microsoft AD
   - Simple AD
   - AD Connector
3. Masukkan informasi direktori.
4. Pilih dua subnet dalam VPC dari dua Availability Zone yang berbeda. Untuk informasi selengkapnya, lihat Mengkonfigurasi VPC dengan subnet publik.

5. Tinjau informasi direktori Anda dan pilih Buat direktori.

Mengkonfigurasi AppStream 2.0 untuk Amazon WorkSpaces Thin Client

AppStream 2.0 instance akan terdaftar berdasarkan nama Stack dan akan memerlukan URL login iDP untuk dikonfigurasi pada halaman create environment. Karena otentikasi SAMP untuk AppStream 2.0 hanya mendukung otentikasi yang dimulai, administrator harus memasukkan URL login yang benar secara manual.

> **Note**
>
> Konfigurasi harus dilakukan sebelum menggunakan konsol untuk pertama kalinya. Anda tidak disarankan memodifikasi fitur prasyarat apa pun setelah Anda mulai menggunakan konsol.

Langkah 1: Verifikasi bahwa sistem Anda memenuhi AppStream 2.0 fitur yang diperlukan

Agar konsol administrator WorkSpaces Thin Client berfungsi dengan AppStream 2.0 dengan benar, sistem Anda harus memenuhi persyaratan spesifik berikut. Tabel ini mencantumkan semua fitur yang didukung ini dan persyaratannya.

Fitur	Persyaratan
Penyedia Identitas	Buka Pengaturan SAMP di Panduan Administrator AppStream 2.0 untuk membuat Penyedia Identitas. Saat diminta untuk Buat konsol env, masukkan URL Login IDP Anda.
Sistem operasi	Windows
Jenis Platform	Windows Server (2012 R2, 2016 atau 2019)
Protokol streaming	Streaming TCP

Fitur	Persyaratan
	Ada mekanisme auto fallback ke TCP jika UDP tidak tersedia.
Salin dan Tempel Lokal	Nonaktifkan Dikonfigurasi pada tingkat tumpukan AppStream 2.0
Berbagi Folder Lokal	Nonaktifkan Dikonfigurasi pada tingkat tumpukan AppStream 2.0
Pencetakan Lokal	Nonaktifkan Dikonfigurasi pada tingkat tumpukan AppStream 2.0

Persyaratan kunci layar melalui otentikasi SAMP pada AppStream 2.0 juga didukung. User Pool dan mekanisme otentikasi Programmatic tidak didukung pada WorkSpaces Thin Client.

Langkah 2: Siapkan tumpukan AppStream 2.0 Anda

Untuk melakukan streaming aplikasi Anda, AppStream 2.0 memerlukan lingkungan yang menyertakan armada yang terkait dengan tumpukan, dan setidaknya satu gambar aplikasi. Ikuti langkah-langkah ini untuk menyiapkan armada dan tumpukan dan memberi pengguna akses ke tumpukan. Jika Anda belum melakukannya, kami sarankan Anda mencoba prosedur di Memulai dengan AppStream 2.0: Mengatur Dengan Aplikasi Sampel.

Jika Anda ingin membuat gambar untuk digunakan, lihat Tutorial: Membuat Gambar AppStream 2.0 Kustom dengan Menggunakan Konsol AppStream 2.0.

Jika Anda berencana untuk menggabungkan armada ke domain Active Directory, konfigurasikan domain Active Directory Anda sebelum menyelesaikan langkah-langkah berikut. Untuk informasi selengkapnya, lihat Menggunakan Active Directory dengan AppStream 2.0.

Tugas

- Buat Armada
- Buat Stack
- Memberikan Akses ke Pengguna
- Bersihkan Sumber Daya

Mengkonfigurasi Amazon WorkSpaces Secure Browser untuk Amazon WorkSpaces Thin Client

Amazon WorkSpaces Secure Browser didasarkan pada titik akhir portal web mereka di halaman lingkungan WorkSpaces Thin Client Create di dalam AWS konsol.

> **Note**
>
> Konfigurasi harus dilakukan sebelum menggunakan konsol untuk pertama kalinya. Anda tidak disarankan memodifikasi fitur prasyarat apa pun setelah Anda mulai menggunakan konsol.

Langkah 1: Verifikasi bahwa sistem Anda memenuhi fitur yang diperlukan Amazon WorkSpaces Secure Browser

Agar Konsol Administrator Klien WorkSpaces Tipis berfungsi dengan baik dengan Amazon WorkSpaces Secure Browser, sistem Anda harus memenuhi persyaratan spesifik berikut. Tabel ini mencantumkan semua fitur yang didukung ini dan persyaratannya.

Fitur	Persyaratan
Salin dan Tempel Lokal	Nonaktifkan
Berbagi Folder Lokal	Nonaktifkan

> **Note**
>
> Ekstensi Browser WorkSpaces Aman untuk sistem masuk tunggal saat ini tidak didukung di WorkSpaces Thin Client.

Langkah 2: Siapkan portal Browser WorkSpaces Aman

WorkSpaces Thin Client bekerja dengan VPC Browser WorkSpaces Aman dalam konfigurasi tertentu:

1. Buat VPC menggunakan template AWS CodeBuild Cloudformation.
2. Siapkan Penyedia Identitas Anda.
3. Buat portal Browser WorkSpaces Aman Amazon.
4. Uji portal Amazon WorkSpaces Secure Browser baru Anda.

Memulai konsol administrator Klien WorkSpaces Tipis

WorkSpaces Thin Client adalah perangkat thin client hemat biaya yang dibangun untuk bekerja dengan layanan AWS End User Computing untuk memberi Anda akses instan yang aman ke aplikasi dan desktop virtual.

Topik

Wilayah Tercakup

WorkSpaces Thin Client tersedia di Wilayah berikut.

Hanya konsol administrator Klien WorkSpaces Tipis yang tersedia di Wilayah ini. WorkSpaces Perangkat Thin Client saat ini hanya tersedia di AS, Jerman, Prancis, Italia, dan Spanyol.

Nama Wilayah	Wilayah	Titik akhir	Tautan konsol
US East (Northern Virginia)	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
AS Barat (Oregon)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
Asia Pasifik (Mumbai)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home
Eropa (Irlandia)	eu-west-1	thinclient.eu-west	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home

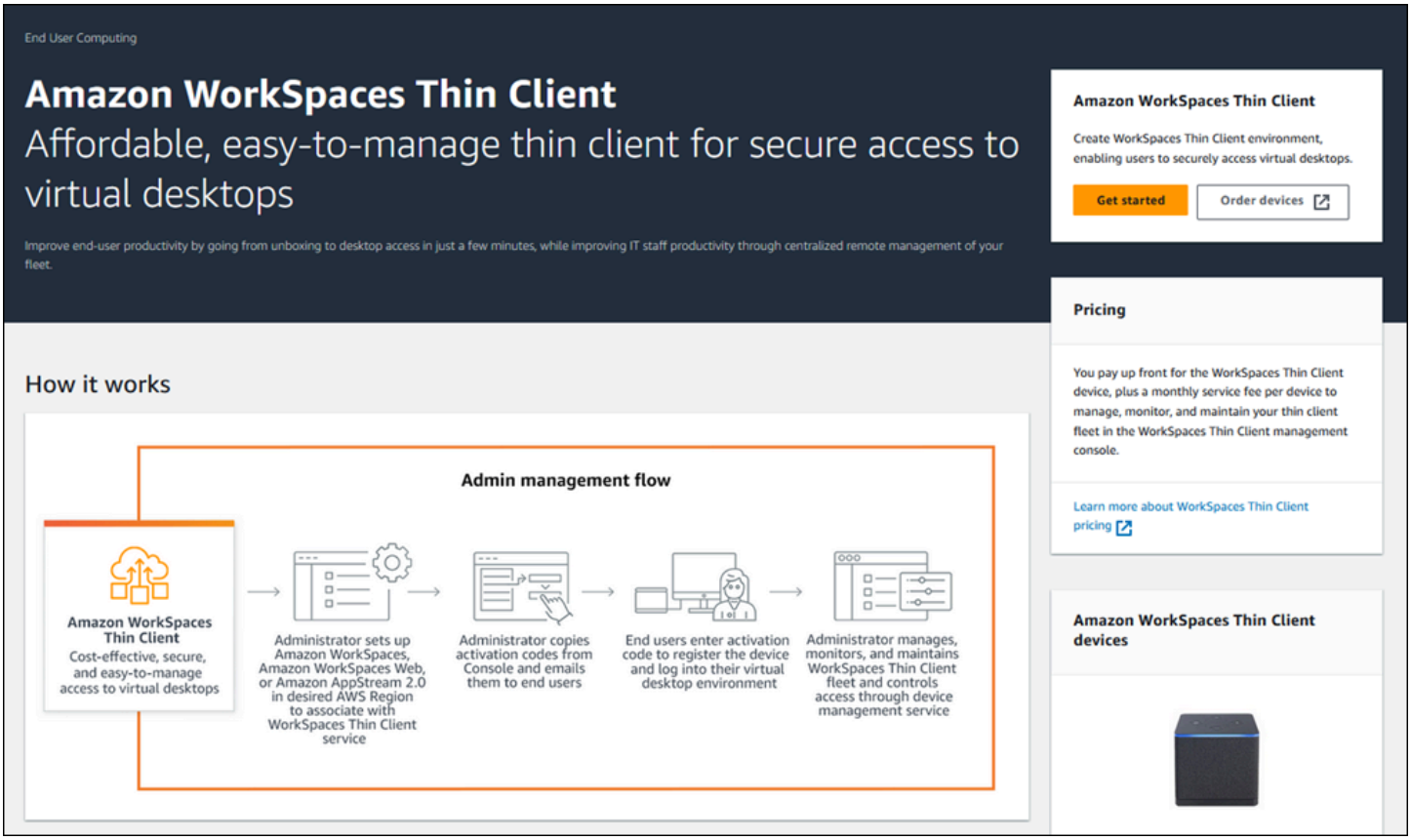
Nama Wilayah	Wilayah	Titik akhir	Tautan konsol
		-1.amazonaws.com	
Kanada (Pusat)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
Eropa (Frankfurt)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
Eropa (London)	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

Meluncurkan konsol administrator WorkSpaces Thin Client

Ketika Anda memiliki AWS akun, Anda dapat meluncurkan konsol administrator dan pergi ke konsol Klien WorkSpaces Tipis. Untuk meluncurkan konsol, lakukan hal berikut:

1. Masuk ke AWS akun Anda.
2. Akses konsol WorkSpaces Thin Client.
3. Pilih Memulai dan Anda akan diarahkan ke Lingkungan.

Menggunakan konsol administrator WorkSpaces Thin Client



Selamat datang di Konsol Administrator Klien WorkSpaces Tipis!

Dari sini, Anda dapat mengelola armada perangkat dan lingkungan WorkSpaces Thin Client untuk tim Anda.

Untuk informasi mengenai perangkat WorkSpaces Thin Client, silakan merujuk ke Panduan Pengguna Klien WorkSpaces Tipis.

Mari kita mulai.

Topik

Lingkungan

Setiap perangkat WorkSpaces Thin Client menggunakan lingkungan desktop virtual individual untuk mengakses sumber daya online-nya. Pengguna mengakses lingkungan ini dengan menggunakan salah satu penyedia desktop virtual berikut:

- Amazon WorkSpaces
- AppStream 2.0
- Browser WorkSpaces Aman Amazon

Daftar lingkungan

Rincian daftar lingkungan

Nama - Pengidentifikasi unik yang terkait dengan lingkungan ini.

Layanan desktop virtual - Penyedia desktop virtual yang digunakan lingkungan ini.

ID layanan desktop virtual - Pengidentifikasi unik yang diberikan penyedia layanan desktop virtual ke lingkungan ini.

Kode aktivasi - Kode yang digunakan oleh pengguna akhir untuk mengakses lingkungan desktop virtual.

Jumlah perangkat - Jumlah perangkat WorkSpaces Thin Client yang mengakses lingkungan ini.

Tindakan daftar lingkungan

Cari - Menelusuri semua lingkungan yang Anda kelola.

Refresh - Menyegarkan daftar lingkungan.

Lihat detail - Menampilkan detail Lingkungan.

Tindakan - Membuka daftar dropdown tempat Anda dapat Mengedit atau Menghapus lingkungan.

Buat lingkungan - Memulai proses menciptakan lingkungan

Buat lingkungan - Memulai proses menciptakan lingkungan.

Topik

Detail Lingkungan

Saat Anda memilih lingkungan, konsol WorkSpaces Thin Client menampilkan detail untuk lingkungan tersebut untuk Anda tinjau. Konsol juga menampilkan detail tentang penyedia desktop virtual yang digunakan lingkungan ini.

Topik

Ringkasan

Nama - Pengidentifikasi unik yang terkait dengan lingkungan ini.

Layanan desktop virtual - Penyedia desktop virtual yang digunakan lingkungan ini.

ID layanan desktop virtual - Pengidentifikasi unik yang diberikan penyedia layanan desktop virtual ke lingkungan ini.

Kode aktivasi - Kode ini digunakan oleh pengguna akhir untuk mengakses lingkungan desktop virtual.

Selalu simpan perangkat lunak up-to-date - Pengaturan ini memungkinkan pembaruan perangkat lunak otomatis.

Waktu mulai jendela pemeliharaan - Waktu setiap minggu ketika pembaruan perangkat lunak otomatis dimulai.

Waktu akhir jendela pemeliharaan - Waktu setiap minggu ketika pembaruan perangkat lunak otomatis selesai.

Jendela pemeliharaan hari dalam seminggu - Hari-hari pembaruan perangkat lunak otomatis terjadi.

Perangkat terkait - Jumlah perangkat WorkSpaces Thin Client yang mengakses lingkungan ini.

Waktu dibuat - Tanggal dan waktu lingkungan ini dibuat.

Detail lingkungan desktop virtual

Detail WorkSpaces direktori Amazon

ID Direktori - WorkSpaces Direktori Amazon yang terkait dengan lingkungan ini.

Nama direktori - Pengidentifikasi unik yang terkait dengan WorkSpaces direktori Amazon ini.

Nama organisasi - Nama organisasi yang mengontrol WorkSpaces direktori Amazon.

Jenis direktori - Format WorkSpaces direktori Amazon.

Terdaftar - Apakah WorkSpaces direktori Amazon ini terdaftar.

Status - Apakah WorkSpaces direktori Amazon ini aktif.

Detail portal Amazon WorkSpaces Secure Browser

Nama - Pengidentifikasi unik yang terkait dengan portal Amazon WorkSpaces Secure Browser ini.

Waktu dibuat - Tanggal dan waktu ketika tumpukan AppStream 2.0 ini dibuat.

Titik akhir portal web - Url yang digunakan untuk mengakses lingkungan desktop virtual Anda.

AppStream 2.0 rincian

Nama tumpukan - Pengidentifikasi unik yang terkait dengan tumpukan AppStream 2.0 ini.

IdP login url - URL penyedia identitas yang digunakan untuk masuk dan keluar dari tumpukan AppStream 2.0 Anda.

Waktu dibuat - Tanggal dan waktu ketika tumpukan AppStream 2.0 ini dibuat.

Pembuatan lingkungan

Untuk memulai, setiap perangkat memerlukan layanan AWS End User Computing. WorkSpaces Thin Client menggunakan layanan berikut:

- Amazon WorkSpaces melalui direktori yang ditetapkan

- AppStream 2.0 melalui tumpukan yang ditugaskan
- Amazon WorkSpaces Secure Browser melalui alamat portal web

Anda harus menetapkan layanan ke lingkungan yang ada atau membuat yang baru.

> **Note**
>
> WorkSpaces Thin Client hanya menampilkan desktop virtual di Wilayah yang sama.

Topik

Langkah 1: Masukkan detail lingkungan Anda

1. Masukkan nama untuk lingkungan Anda di bidang Detail lingkungan.
2. Untuk mengatur patch perangkat lunak otomatis, centang kotak untuk Selalu simpan perangkat lunak up-to-date.

   > **Note**
   >
   > Jika pembaruan perangkat lunak otomatis tidak diaktifkan, perangkat yang terdaftar di lingkungan ini tidak akan menerima pembaruan perangkat lunak sampai Anda mendorong pembaruan secara manual atau ketika perangkat lunak mencapai kedaluwarsa dan sistem memaksa pembaruan.
   > Juga, versi Perangkat Lunak Set ditentukan oleh sistem. Versi ini mungkin bukan yang terbaru.

3. Pilih kapan Anda ingin menjadwalkan jendela pemeliharaan untuk lingkungan Anda.

   - Terapkan jendela pemeliharaan luas sistem - Secara otomatis memperbarui perangkat lunak lingkungan pada waktu yang ditentukan setiap minggu.
   - Terapkan jendela pemeliharaan khusus - Tetapkan hari dan waktu ketika Anda ingin perangkat lunak lingkungan diperbarui setiap minggu.

4. Pilih layanan desktop virtual.

   - Amazon WorkSpaces
   - Browser WorkSpaces Aman Amazon
   - AppStream 2.0

Langkah 2: Pilih penyedia desktop virtual Anda

Anda harus memiliki layanan untuk memberi pengguna Anda akses ke desktop virtual dan sumber daya yang kompatibel.

> **Important**
>
> Agar Konsol Administrator Klien WorkSpaces Tipis berfungsi dengan baik, sistem Anda harus memenuhi persyaratan tertentu. Persyaratan ini tercantum dalam Prasyarat dan Konfigurasi. Pastikan sistem Anda memenuhi persyaratan ini sebelum menyiapkan konsol.

Menggunakan Amazon WorkSpaces

Amazon WorkSpaces adalah layanan virtualisasi desktop yang dikelola sepenuhnya untuk Windows yang memungkinkan Anda mengakses sumber daya dari perangkat apa pun yang didukung.

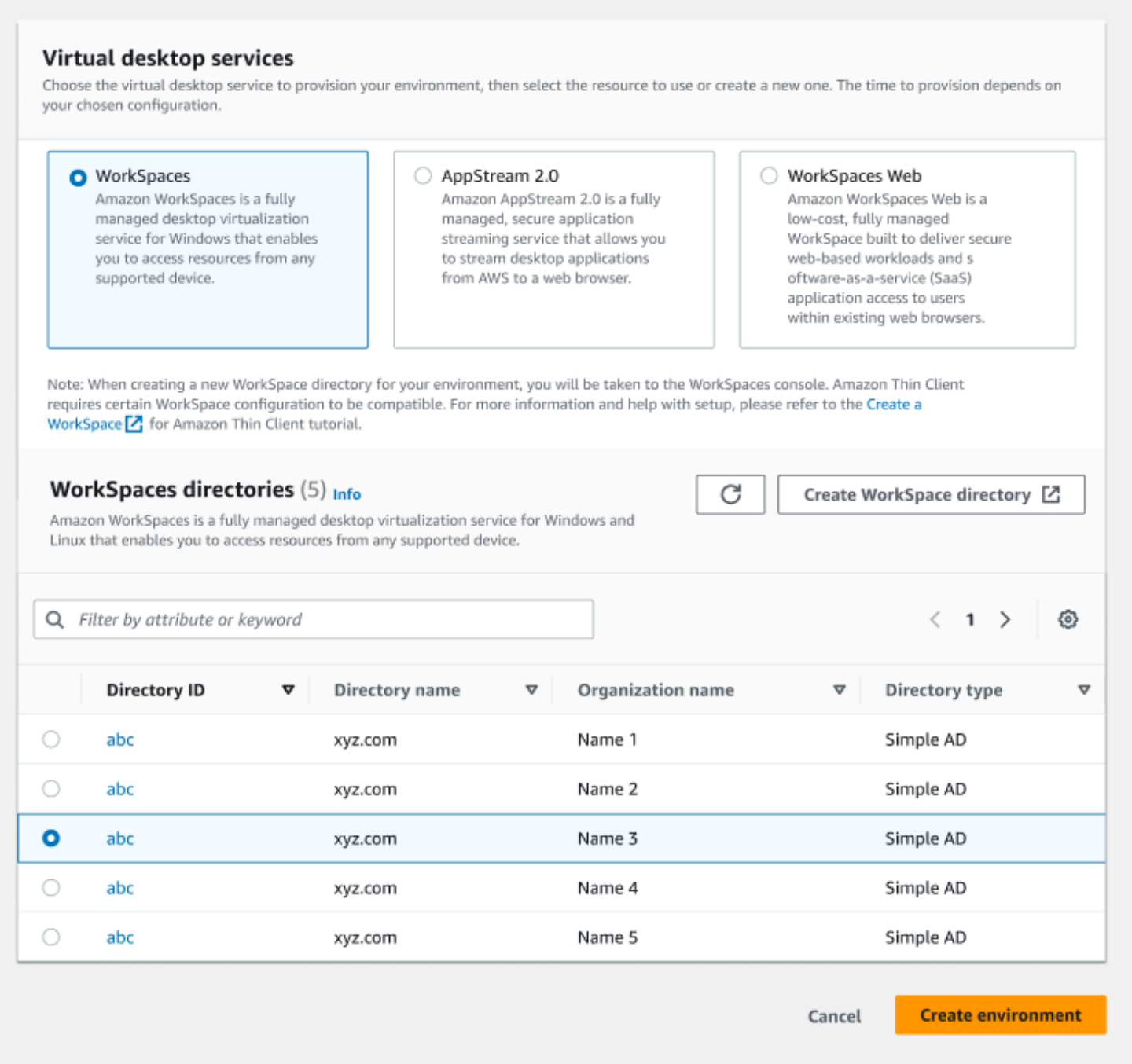
1. Untuk menggunakan Amazon WorkSpaces, lakukan salah satu hal berikut:

   - Pilih direktori yang ingin Anda gunakan untuk lingkungan Anda. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari direktori dengan menggunakan bidang pencarian.

     > **Note**
     >
     > Jika Anda tidak melihat direktori yang ada dalam daftar, verifikasi di Konsol WorkSpaces Manajemen bahwa direktori tersebut memenuhi persyaratan Klien WorkSpaces Tipis.

   - Buat direktori dengan memilih tombol Buat WorkSpaces direktori. Untuk informasi selengkapnya tentang membuat WorkSpaces direktori, lihat Mengelola direktori untuk. WorkSpaces

2. Pilih tombol Buat lingkungan.



Saat Anda membuat lingkungan, Anda masih dapat mengedit detailnya nanti. Untuk informasi selengkapnya, lihat Mengedit lingkungan.

Menggunakan AppStream 2.0

AppStream 2.0 adalah layanan streaming aplikasi yang dikelola sepenuhnya dan aman yang dapat Anda gunakan untuk melakukan streaming aplikasi desktop dari AWS ke browser web.

> **Warning**
>
> Untuk membuat lingkungan AppStream 2.0, Anda harus `cli_follow_urlparam` mengatur ke`false`. Untuk mencapai ini, lakukan hal berikut:
>
> - Untuk profil default, jalankan`aws configure set cli_follow_urlparam false`.
> - Untuk profil dengan nama`ProfileName`, jalankan`aws configure set cli_follow_urlparam false --profile ProfileName`.

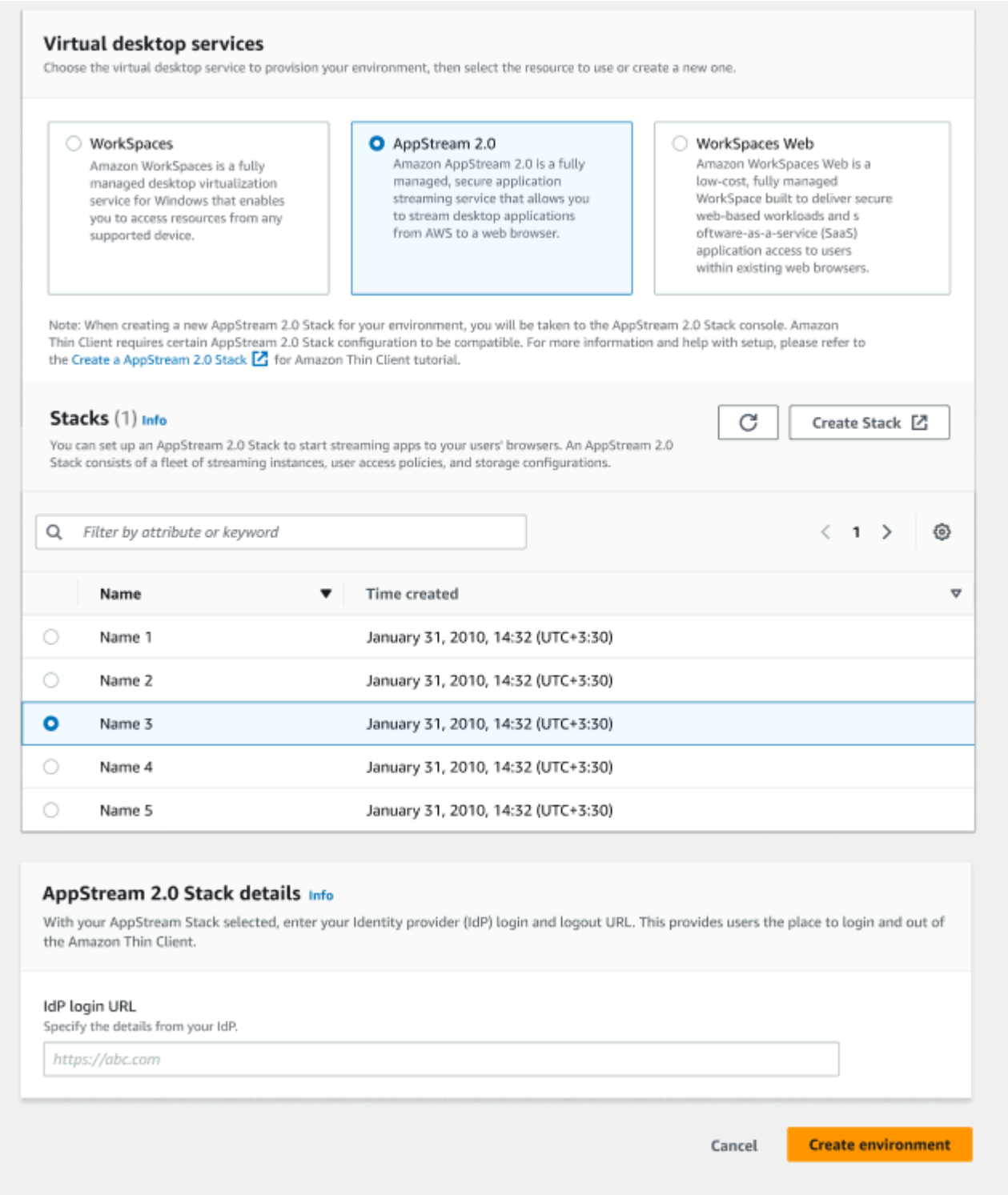
1. Untuk mengatur AppStream 2.0, lakukan salah satu hal berikut:

   - Pilih tumpukan yang ingin Anda gunakan untuk lingkungan Anda. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari tumpukan dengan menggunakan bidang pencarian.

     > **Note**
     >
     > Jika Anda tidak melihat tumpukan yang ada di daftar, verifikasi di Konsol Manajemen AppStream 2.0 bahwa tumpukan tersebut memenuhi persyaratan Klien WorkSpaces Tipis.

   - Buat tumpukan dengan memilih tombol Create Stack. Untuk informasi selengkapnya tentang membuat tumpukan AppStream 2.0, lihat Membuat Tumpukan.

2. Masukkan URL login dan logout penyedia identitas Anda di kolom URL login iDP. Ini memberi pengguna tempat untuk masuk dan keluar dari WorkSpaces Thin Client.
3. Pilih tombol Buat lingkungan.



Setelah Anda membuat lingkungan Anda, Anda masih dapat mengedit detailnya nanti. Untuk informasi selengkapnya, lihat Mengedit lingkungan.

Menggunakan Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser adalah WorkSpaces konsol berbiaya rendah dan terkelola penuh yang dibangun untuk memberikan beban kerja berbasis web yang aman dan akses aplikasi perangkat lunak sebagai layanan (SaaS) ke pengguna dalam browser web yang ada.

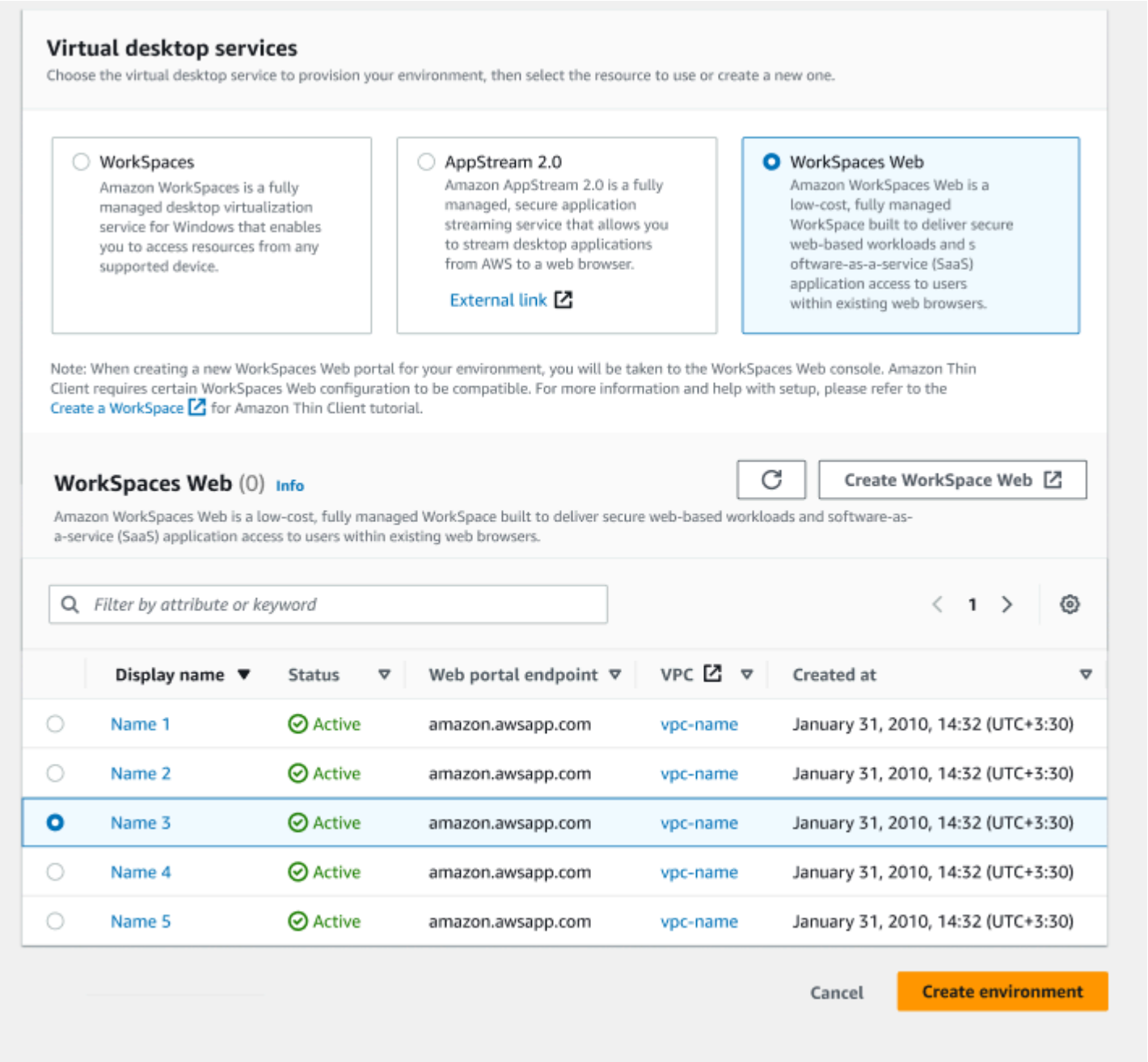
1. Untuk menyiapkan Amazon WorkSpaces Secure Browser, lakukan salah satu hal berikut:

   - Pilih portal web yang ingin Anda gunakan untuk lingkungan Anda. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari portal web dengan menggunakan bidang pencarian.

     > **Note**
     >
     > Jika Anda tidak melihat portal web yang ada dalam daftar, verifikasi di Konsol Manajemen Browser WorkSpaces Aman bahwa portal tersebut memenuhi persyaratan Klien WorkSpaces Tipis.

   - Buat portal web dengan memilih tombol Create WorkSpaces Secure Browser. Untuk informasi selengkapnya tentang membuat portal web Browser WorkSpaces Aman, lihat Menyiapkan Browser WorkSpaces Aman Amazon.

2. Pilih tombol Buat lingkungan.



Setelah Anda membuat lingkungan Anda, Anda masih dapat mengedit detailnya nanti. Untuk informasi selengkapnya, lihat Mengedit lingkungan.

Langkah 3: Kirim kode aktivasi ke pengguna perangkat Anda

Setelah mengatur lingkungan dan layanan desktop virtual, Anda akan menerima kode aktivasi unik untuk penyiapan Anda di AWS Management Console.

Berikan kode aktivasi ini kepada pengguna perangkat WorkSpaces Thin Client mana pun, dan mereka dapat menggunakannya untuk mengakses desktop virtual mereka.

Lihat Panduan Pengguna Klien WorkSpaces Tipis untuk informasi tambahan tentang cara membantu pengguna perangkat mengatur Amazon WorkSpaces Thin Client mereka.

Mengedit lingkungan

Konsol administrasi Klien WorkSpaces Tipis mengelola lingkungan desktop virtual untuk pengguna individu. Dari konsol ini, Anda dapat mengedit atau menghapus lingkungan desktop virtual.

1. Pilih lingkungan yang ingin Anda edit.

   > **Note**
   >
   > Anda dapat menelusuri daftar dropdown atau Anda dapat mencari lingkungan dengan menggunakan bidang pencarian.

2. Pilih tombol Tindakan.
3. Pilih Edit dari daftar dropdown. Anda akan diarahkan ke jendela Edit lingkungan.
4. Edit salah satu dari berikut ini:
   - Ubah nama lingkungan Anda di bidang Nama Lingkungan.
   - Ubah kotak centang untuk detail pembaruan perangkat lunak untuk pembaruan patch perangkat lunak otomatis.
   - Ubah saat Anda ingin menjadwalkan jendela pemeliharaan untuk lingkungan Anda.
5. Pilih tombol Edit lingkungan.

Menghapus lingkungan

> **Note**
>
> Anda tidak dapat menghapus lingkungan jika memiliki perangkat yang terdaftar di dalamnya. Pertama, Anda harus membatalkan pendaftaran dan menghapus semua perangkat di lingkungan.

1. Pilih lingkungan yang ingin Anda hapus. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari lingkungan dengan menggunakan bidang pencarian.
2. Pilih tombol Tindakan.
3. Pilih Hapus dari daftar dropdown. Jendela konfirmasi lingkungan Hapus muncul.
4. Ketik “hapus” di bidang konfirmasi.
5. Pilih tombol Hapus.

Perangkat

Setiap pengguna akhir WorkSpaces Thin Client memiliki perangkat khusus yang menghubungkan mereka ke lingkungan desktop virtual dan sumber daya online mereka. Perangkat ini dikelola melalui konsol administrator Klien WorkSpaces Tipis di AWS situs.

Dari konsol ini, Anda dapat memesan perangkat untuk tim Anda.

Daftar perangkat

Detail daftar perangkat

ID Perangkat - Nomor identifikasi yang ditetapkan untuk perangkat individual.

Nama perangkat - (opsional) Nama unik yang Anda berikan ke perangkat.

Status aktivitas - Status perangkat saat ini. Ada dua status status:

- Aktif - Terhubung ke jaringan setidaknya sekali dalam tujuh hari terakhir.
- Tidak aktif - Tidak terhubung ke jaringan dalam tujuh hari terakhir.

Status pendaftaran - Konfirmasi bahwa perangkat telah disiapkan, dikaitkan dengan AWS akun ini, dan merupakan bagian dari lingkungan tertentu. Itu bisa di salah satu negara berikut:

- Terdaftar - Ini adalah status default.
- Deregistering - Perangkat sedang dalam proses Reset dan Deregister.

> **Note**
>
> Anda dapat menghapus perangkat jika dalam keadaan deregistering.

- Deregsitered - Perangkat telah berhasil dideregistrasi.

> **Note**
>
> Anda hanya dapat menghapus perangkat jika dalam status Deregistering atau Deregistered.

- Diarsipkan - Perangkat diarsipkan.

ID Lingkungan - Pengidentifikasi lingkungan tempat perangkat ini terpasang.

Kepatuhan perangkat lunak - Status kepatuhan perangkat lunak perangkat. Ada dua status status:

- Patuh
- Tidak patuh

Tindakan daftar perangkat

Cari - Menelusuri semua perangkat yang Anda kelola.

Refresh - Menyegarkan daftar perangkat.

Lihat detail - Menampilkan detail Perangkat.

Tindakan - Membuka daftar dropdown di mana Anda dapat melakukan hal berikut:

- Edit nama perangkat
- Deregister
- Arsip
- Hapus
- Ekspor detail perangkat

Perangkat pesanan - Memulai proses pemesanan perangkat.

Topik

- Detail perangkat
- Mengedit nama perangkat

- Menyetel ulang dan membatalkan pendaftaran perangkat
- Mengarsipkan perangkat
- Menghapus perangkat
- Mengekspor detail perangkat

Detail perangkat

Ringkasan

Nomor seri perangkat - Nomor identifikasi yang ditetapkan untuk perangkat individual.

ARN - Pengidentifikasi unik untuk perangkat dalam format Amazon Resource Name (ARN).

Nama perangkat - Nama yang Anda berikan ke perangkat. Jika Anda belum membuat nama, Anda dapat menamainya, atau itu akan mendapatkan nama default.

Jenis perangkat - Jenis perangkat pengguna akhir yang ditautkan ke akun.

Status aktivitas - Status saat ini dari perangkat ini. Dua status status tersebut adalah:

- Aktif
- Nonaktif

ID Lingkungan - Nomor identifikasi lingkungan yang digunakan perangkat.

Status pendaftaran - Konfirmasi bahwa perangkat telah disiapkan, dikaitkan dengan AWS akun ini, dan merupakan bagian dari lingkungan tertentu. Itu bisa di salah satu dari empat negara berikut:

- Terdaftar - Ini adalah status default.
- Deregistering - Perangkat sedang dalam proses Reset dan Deregister.
- Deregistrasi - Perangkat telah berhasil dideregistrasi.

> **Note**
>
> Anda hanya dapat menghapus perangkat jika berada dalam status Deregistered atau Diarsipkan.

- Diarsipkan - Perangkat ini telah ditandai oleh administrator sebagai tidak sedang dalam layanan.

Terdaftar sejak - Tanggal perangkat diaktifkan.

Terakhir masuk - Tanggal dan waktu login terbaru.

Postur terakhir diperiksa di - Tanggal dan waktu check-in perangkat terbaru.

Versi perangkat lunak saat ini - Versi perangkat lunak yang saat ini digunakan perangkat ini.

Dijadwalkan untuk pembaruan perangkat lunak - Versi perangkat lunak terjadwal pada perangkat.

Kepatuhan perangkat lunak - Konfirmasi bahwa perangkat lunak tersebut valid. Ada dua status status:

- Patuh
- Tidak Patuh

Log pengguna

Akses perangkat terakhir - Tanggal dan waktu saat perangkat ini terakhir digunakan.

Mengedit nama perangkat

1. Pilih perangkat yang ingin Anda edit. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari perangkat dengan menggunakan bidang pencarian.
2. Pilih tombol Tindakan.
3. Pilih Edit nama perangkat dari daftar tarik-turun. Jendela Edit nama perangkat muncul.
4. Masukkan nama perangkat baru di bidang Konfirmasi nama perangkat.
5. Pilih tombol Simpan.

Menyetel ulang dan membatalkan pendaftaran perangkat

1. Pilih perangkat yang ingin Anda deregister. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari perangkat dengan menggunakan bidang pencarian.
2. Pilih tombol Tindakan.
3. Pilih Deregister dari daftar dropdown. Jendela Deregister muncul.
4. Masukkan “deregister” di bidang konfirmasi.
5. Pilih tombol Deregister.

> **Note**
>
> Deregistering secara paksa log out pengguna dan memerlukan reboot perangkat WorkSpaces Thin Client mereka di tengah sesi.

Mengarsipkan perangkat

1. Pilih perangkat yang ingin Anda arsipkan. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari perangkat dengan menggunakan bidang pencarian.
2. Pilih tombol Tindakan.
3. Pilih Arsip dari daftar dropdown. Jendela Arsip muncul.
4. Masukkan “reset dan arsipkan” di bidang konfirmasi.
5. Pilih tombol Reset dan Arsipkan.

> **Note**
>
> Mengarsipkan perangkat secara paksa mengeluarkan pengguna dan memerlukan reboot perangkat WorkSpaces Thin Client mereka di tengah sesi.

Menghapus perangkat

1. Pilih perangkat yang ingin Anda hapus. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari perangkat dengan menggunakan bidang pencarian.
2. Pilih tombol Tindakan.
3. Pilih Hapus dari daftar dropdown. Jendela Hapus muncul.
4. Masukkan “hapus” di bidang konfirmasi.
5. Pilih tombol Hapus.

> **Note**
>
> Ketika perangkat telah berhasil dihapus, pengguna harus mengembalikan perangkat WorkSpaces Thin Client kembali ke Amazon.

Mengekspor detail perangkat

1. Pilih perangkat dari mana Anda ingin mengekspor detailnya. Anda dapat menelusuri daftar dropdown atau Anda dapat mencari perangkat dengan menggunakan bidang pencarian.
2. Pilih tombol Tindakan.
3. Pilih Ekspor detail perangkat dari daftar tarik-turun. Detail untuk unduhan perangkat yang dipilih dalam format spreadsheet.

Pembaruan perangkat lunak

WorkSpaces Thin Client terkadang memerlukan pembaruan perangkat lunak yang memperkenalkan fungsionalitas baru dan menerapkan patch keamanan. Pembaruan ini diwakili oleh perangkat lunak berversi.

Perangkat Lunak dapat berisi pembaruan ke aplikasi perangkat lunak atau sistem operasi untuk perangkat WorkSpaces Thin Client. Dari konsol ini, Anda dapat memilih untuk memperbarui perangkat lunak segera atau Anda dapat menjadwalkan pembaruan otomatis selama jendela pemeliharaan untuk lingkungan.

Lihat set perangkat lunak lingkungan Klien WorkSpaces Tipis untuk daftar Set Perangkat Lunak yang dirilis.

Topik

- Memperbarui perangkat lunak lingkungan
- Memperbarui perangkat lunak perangkat
- WorkSpaces Rilis perangkat lunak Thin Client

Memperbarui perangkat lunak lingkungan

WorkSpaces Thin Client adalah layanan AWS End User Computing yang menyediakan akses pengguna ke desktop virtual. Desktop virtual ini diperbarui secara berkala dengan perangkat lunak baru. Untuk memperbarui perangkat lunak lingkungan, lakukan hal berikut:

1. Pilih perangkat lunak yang ditetapkan dari daftar di Pembaruan perangkat lunak yang tersedia. Untuk daftar perangkat lunak, lihat set perangkat lunak lingkungan WorkSpaces Thin Client.
2. Pilih tombol Instal.

3. Pilih Lingkungan di bagian atas halaman.
4. Pilih lingkungan yang akan diperbarui dari daftar di bagian Lingkungan.
5. Pilih kapan harus memperbarui lingkungan di Jadwalkan pembaruan dengan memilih salah satu dari berikut ini:

   - Perbarui perangkat lunak sekarang - Memulai pembaruan perangkat lunak lingkungan pada semua perangkat terdaftar.

     > **Note**
     >
     > Memperbarui perangkat lunak sekarang dapat mengganggu sesi pengguna aktif apa pun.

   - Perbarui perangkat lunak selama setiap jendela pemeliharaan lingkungan - Memperbarui perangkat lunak lingkungan selama jendela pemeliharaan terjadwal untuk lingkungan.
6. Centang kotak untuk mengotorisasi pembaruan. Kotak ini harus dicentang agar perangkat lunak dapat diperbarui.
7. Pilih tombol Instal.

Memperbarui perangkat lunak perangkat

WorkSpaces Thin Client adalah layanan AWS End User Computing yang menyediakan perangkat thin client yang menghubungkan pengguna ke desktop virtual khusus. Perangkat ini diperbarui secara berkala dengan perangkat lunak baru. Untuk memperbarui perangkat lunak perangkat, lakukan hal berikut:

1. Pilih perangkat lunak yang ditetapkan dari daftar di Pembaruan perangkat lunak yang tersedia.
2. Pilih tombol Instal.
3. Pilih Perangkat di bagian atas halaman.
4. Pilih perangkat atau perangkat yang akan diperbarui dari daftar di bagian Perangkat. Untuk daftar perangkat lunak, lihat set perangkat lunak lingkungan WorkSpaces Thin Client.
5. Pilih kapan harus memperbarui lingkungan dari opsi Jadwalkan pembaruan dengan memilih salah satu dari berikut ini:

   - Perbarui perangkat lunak sekarang - Segera perbarui perangkat lunak perangkat.

> **Note**
>
> Memperbarui perangkat lunak sekarang dapat mengganggu sesi pengguna aktif apa pun.

- Perbarui perangkat lunak selama setiap jendela pemeliharaan perangkat - Memperbarui perangkat lunak lingkungan selama jendela pemeliharaan terjadwal untuk perangkat.

6. Centang kotak untuk mengotorisasi pembaruan. Kotak ini harus dicentang agar perangkat lunak dapat diperbarui.
7. Pilih tombol Instal.

WorkSpaces Rilis perangkat lunak Thin Client

WorkSpaces Thin Client adalah layanan AWS End User Computing yang menyediakan pengguna akses ke desktop virtual pada perangkat. Perangkat ini diperbarui secara berkala dengan perangkat lunak baru. Tabel berikut menjelaskan semua set perangkat lunak yang dirilis. Administrator dapat menggunakan konsol AWS manajemen untuk melihat set perangkat lunak yang tersedia.

Set perangkat lunak	Tanggal rilis	Perubahan
2.5.0	06-13-2024	• Memperbaiki masalah saat perangkat menunjukkan layar pengaturan keyboard dan mouse sebentar saat bangun dari tidur sebelum meluncurkan sesi. • Tombol Beranda pada toolbar perangkat diubah namanya menjadi Masuk. • Perbaikan kinerja panggilan audio/video dalam sesi.
2.4.3	05-29-2024	• Perbaikan zero-day untuk masalah keamanan kritis CVE-2024-5274 Chromium.

Set perangkat lunak	Tanggal rilis	Perubahan
2.4.2	05-17-2024	• Perbaikan zero-day untuk masalah keamanan kritis CVE-2024-4947 Chromium.
2.4.1	05-15-2024	• Perbaikan zero-day untuk masalah keamanan kritis CVE-2024-4671 dan CVE-2024-4761 Chromium. • Memperbaiki masalah yang memungkinkan mengklik kanan tautan AWS dan Privasi di halaman WorkSpaces masuk untuk membuka browser dalam mode yang berdiri sendiri.
2.4.0	05-09-2024	• Memperbaiki masalah yang memblokir “accounts .google.com” dan mencegah penggunaan Google Workspace sebagai IDP untuk sesi 2.0. AppStream • Bilah alat pengaturan perangkat secara otomatis runtuh dengan klik di area mana pun di layar.

Set perangkat lunak	Tanggal rilis	Perubahan
2.3.0	04-05-2024	• Pengaturan perangkat muncul di bilah alat yang diciutkan yang memungkinkan pemanfaatan layar yang terlihat dengan lebih baik. • Pengguna akhir sekarang dapat mengonfigurasi durasi untuk menunggu sebelum perangkat tidur saat tidak aktif. • Memperbaiki masalah di mana URL “about:blank” muncul di tampilan kedua. • Memperbaiki masalah yang mengakibatkan layar putih saat tampilan diperpanjang ditutup. • Level volume yang ditetapkan oleh pengguna akhir sekarang tetap ada di seluruh perangkat restart.
2.2.1	02-16-2024	• Memperbaiki masalah yang terjadi selama proses masuk yang mencegah pengguna masuk ke yang WorkSpaces dikonfigurasi dengan otentikasi SAM 2.0.
2.2.0	02-08-2024	• Menambahkan dukungan untuk keyboard ISO dengan bahasa Inggris (Inggris), Prancis, Jerman, Italia, Spanyol lokal.

Set perangkat lunak	Tanggal rilis	Perubahan
2.1.2	01-26-2024	• Perbaikan zero-day untuk masalah keamanan kritis CVE-2024-0519 Chromium. • Peningkatan latensi pengguna akhir yang terkait dengan fungsionalitas Kunci. • Titik akhir yang menghadap perangkat internal dialihkan ke domain 'thinclient* '.
2.1.1	12-21-2023	• Perbaikan zero-day untuk masalah keamanan kritis CVE-2023-7024 Chromium.
2.1.0	12-20-2023	• Menambahkan tombol Home ke pengaturan perangkat dan memungkin kan dukungan untuk tombol Meta. Hal ini memungkin kan pengguna akhir untuk memanggil layar kunci dengan menekan Meta+L.
2.0.1	12-06-2023	• Perbaikan zero-day untuk masalah keamanan kritis CVE-2024-6345 Chromium.
2.0.0	11-15-2023	• Rilis awal

Menggunakan tag pada sumber daya WorkSpaces Thin Client

Anda dapat mengatur dan mengelola sumber daya untuk Klien WorkSpaces Tipis Anda dengan menetapkan metadata Anda sendiri ke setiap sumber daya sebagai tag. Anda menentukan kunci dan nilai untuk setiap tanda. Kunci dapat berupa kategori umum, seperti "proyek," "pemilik," atau "lingkungan," dengan nilai terkait tertentu. Anda dapat menggunakan tag sebagai cara sederhana namun ampuh untuk mengelola sumber daya AWS dan mengatur data, termasuk data penagihan.

Ketika Anda menambahkan tanda ke sumber daya yang ada, tanda tersebut tidak muncul dalam laporan alokasi biaya hingga hari pertama bulan berikutnya. Misalnya, jika Anda menambahkan tag ke perangkat Klien WorkSpaces Tipis yang ada pada 15 Juli, tag tidak akan muncul dalam laporan alokasi biaya hingga 1 Agustus. Untuk informasi selengkapnya, lihat Menggunakan Tag Alokasi Biaya di Panduan Pengguna Penagihan AWS.

> **Note**
>
> Untuk melihat tag sumber daya Klien WorkSpaces Tipis Anda di Cost Explorer, Anda harus mengaktifkan tag yang telah Anda terapkan ke sumber daya Klien WorkSpaces Tipis Anda dengan mengikuti petunjuk dalam Mengaktifkan Tag Alokasi Biaya yang Ditentukan Pengguna di Panduan Pengguna.AWS Billing
> Tag muncul 24 jam setelah aktivasi, tetapi dapat memakan waktu 4-5 hari agar nilai yang terkait dengan tag tersebut muncul di Cost Explorer. Selain itu, untuk menampilkan dan menyediakan data biaya di Cost Explorer, sumber daya WorkSpaces Thin Client yang telah ditandai harus dikenakan biaya selama waktu tersebut. Cost Explorer hanya menampilkan data biaya sejak tag diaktifkan. Tidak ada data riwayat yang tersedia saat ini.

Sumber daya yang dapat Anda tag:

- Anda dapat menambahkan tag ke sumber daya berikut saat Anda membuatnya— Lingkungan Klien WorkSpaces Tipis.
- Anda dapat menambahkan tag ke sumber daya yang ada dari jenis berikut— Lingkungan Klien WorkSpaces Tipis, perangkat, dan set perangkat lunak.

Batasan tag

- Jumlah maksimum tanda per sumber daya—50
- Panjang kunci maksimum—128 karakter Unicode
- Panjang nilai maksimum—256 karakter Unicode
- Kunci dan nilai tag peka huruf besar dan kecil. Karakter yang diperbolehkan adalah: huruf, spasi, dan angka yang dapat mewakili dalam UTF-8, serta karakter berikut: + - = . _ : / @. _:/@. Jangan gunakan spasi terkemuka atau paling belakang.
- Jangan gunakan `aws:` awalan dalam nama atau nilai tag Anda karena itu dicadangkan untuk AWS digunakan. Anda tidak dapat mengedit atau menghapus nama atau nilai tanda dengan prefiks ini.

Untuk memperbarui tag untuk lingkungan yang ada dengan menggunakan konsol

1. Buka konsol WorkSpaces Thin Client.
2. Pilih Lingkungan untuk membuka halaman detailnya
3. Pilih Edit.
4. Di bagian Tag, lakukan satu atau beberapa hal berikut:.
   - Untuk menambahkan tanda, pilih Tambahkan tanda baru lalu edit nilai Kunci dan Nilai.
   - Untuk memperbarui tag, edit nilai Nilai.
   - Untuk menghapus tag, pilih Hapus di sebelah tag.
5. Setelah selesai memperbarui tag, pilih Simpan.

Untuk memperbarui tag untuk perangkat yang ada dengan menggunakan konsol

1. Buka konsol WorkSpaces Thin Client.
2. Pilih perangkat untuk membuka halaman detailnya.
3. Pilih Tanda.
4. Pilih Kelola tanda.
5. Lakukan salah satu atau beberapa hal berikut:
   - Untuk menambahkan tanda, pilih Tambahkan tanda baru lalu edit nilai Kunci dan Nilai.
   - Untuk memperbarui tag, edit nilai Nilai.
   - Untuk menghapus tag, pilih Hapus di sebelah tag.

6. Setelah selesai memperbarui tag, pilih Simpan.

Untuk memperbarui tag untuk pembaruan perangkat lunak dengan menggunakan konsol

1. Buka konsol WorkSpaces Thin Client.
2. Pilih pembaruan Perangkat Lunak untuk membuka halaman detailnya.
3. Di bagian Tag, pilih Kelola tag.
4. Lakukan salah satu atau beberapa hal berikut:
   - Untuk menambahkan tanda, pilih Tambahkan tanda baru lalu edit nilai Kunci dan Nilai.
   - Untuk memperbarui tag, edit nilai Nilai.
   - Untuk menghapus tag, pilih Hapus di sebelah tag.
5. Setelah selesai memperbarui tag, pilih Simpan.

Keamanan di Amazon WorkSpaces Thin Client

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

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

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

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

Topik

Perlindungan data di Amazon WorkSpaces Thin Client

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon WorkSpaces Thin Client. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk

melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. 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, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan 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 pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat 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 Thin Client atau lainnya Layanan AWS menggunakan konsol, API AWS 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.

Amazon WorkSpaces Thin Client mengumpulkan dan memberikan informasi tentang penggunaan pengguna perangkat WorkSpaces Thin Client dan interaksinya dengan layanan desktop virtual.

Misalnya, memori yang tersedia, diagnostik jaringan, informasi jaringan, konektivitas perangkat, kredensyal SAMP, informasi identifikasi perangkat, dan laporan kerusakan. Informasi ini digunakan untuk memberi Anda layanan dan dapat digunakan untuk meningkatkan pengalaman pengguna dengan layanan. Selanjutnya, semata-mata untuk menyediakan layanan kepada Anda, informasi tersebut dapat ditransfer ke luar AWS Wilayah tempat pengguna menggunakan Layanan. Kami memproses informasi ini sesuai dengan Pemberitahuan AWS Privasi.

Topik

Enkripsi data

WorkSpaces Thin Client mengumpulkan data kustomisasi lingkungan dan perangkat, seperti pengaturan pengguna, pengidentifikasi perangkat, informasi penyedia identitas, dan pengenal desktop streaming. WorkSpaces Thin Client juga mengumpulkan stempel waktu sesi. Data yang dikumpulkan disimpan di Amazon DynamoDB dan Amazon S3. WorkSpaces Thin Client menggunakan AWS Key Management Service (KMS) untuk enkripsi.

Untuk mengamankan konten Anda, ikuti panduan ini:

- Terapkan akses hak istimewa paling sedikit dan buat peran khusus yang akan digunakan untuk tindakan Klien WorkSpaces Tipis.
- Lindungi data end-to-end dengan menyediakan kunci yang dikelola pelanggan, sehingga WorkSpaces Thin Client dapat mengenkripsi data Anda saat istirahat dengan kunci yang Anda berikan.
- Hati-hati dengan berbagi kode aktivasi lingkungan dan kredensyal pengguna:
  - Admin diminta untuk masuk ke konsol WorkSpaces Thin Client, dan pengguna diharuskan untuk memberikan kode aktivasi untuk penyiapan WorkSpaces Thin Client menggunakan kredensil untuk masuk ke desktop streaming.
  - Siapa pun yang memiliki akses fisik dapat mengatur Klien WorkSpaces Tipis, tetapi mereka tidak dapat memulai sesi kecuali mereka memiliki kode aktivasi yang valid dan kredensi pengguna untuk masuk.

- Pengguna dapat secara eksplisit mengakhiri sesi mereka dengan memilih untuk mengunci layar mereka, reboot, atau mematikan perangkat dengan menggunakan toolbar perangkat. Ini membuang sesi perangkat dan menghapus kredensyal sesi.

WorkSpaces Thin Client mengamankan konten dan metadata secara default dengan mengenkripsi semua data sensitif dengan KMS. AWS Jika ada kesalahan saat menerapkan pengaturan yang ada, pengguna tidak dapat mengakses sesi baru dan perangkat tidak dapat menerapkan pembaruan perangkat lunak.

Enkripsi data saat istirahat untuk Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client menyediakan enkripsi secara default untuk melindungi data pelanggan sensitif saat istirahat dengan menggunakan kunci enkripsi yang AWS dimiliki.

- AWS kunci yang dimiliki - Amazon WorkSpaces Thin Client menggunakan kunci ini secara default untuk secara otomatis mengenkripsi data yang dapat diidentifikasi secara pribadi. Anda tidak dapat melihat, mengelola, atau menggunakan kunci yang AWS dimiliki atau mengaudit penggunaannya. Namun, Anda tidak perlu mengambil tindakan apa pun atau mengubah program apa pun untuk melindungi kunci yang mengenkripsi data Anda. Untuk informasi selengkapnya, lihat kunci yang AWS dimiliki di Panduan Pengembang Layanan Manajemen AWS Kunci.

Enkripsi data saat istirahat secara default membantu mengurangi overhead operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Pada saat yang sama, ini memungkinkan Anda untuk membangun aplikasi aman yang memenuhi kepatuhan enkripsi yang ketat dan persyaratan peraturan.

Meskipun Anda tidak dapat menonaktifkan lapisan enkripsi ini atau memilih jenis enkripsi alternatif, Anda dapat menambahkan lapisan enkripsi kedua di atas kunci enkripsi milik AWS yang ada dengan memilih kunci yang dikelola pelanggan saat Anda membuat Lingkungan Klien Tipis:

- Kunci terkelola pelanggan — Amazon WorkSpaces Thin Client mendukung penggunaan kunci terkelola pelanggan simetris yang Anda buat, miliki, dan kelola untuk menambahkan enkripsi lapisan kedua pada enkripsi AWS milik yang ada. Karena Anda memiliki kontrol penuh atas lapisan enkripsi ini, Anda dapat melakukan tugas-tugas seperti berikut:
  - Menetapkan dan memelihara kebijakan utama
  - Menetapkan dan memelihara kebijakan dan hibah IAM
  - Mengaktifkan dan menonaktifkan kebijakan utama

- Memutar bahan kriptografi kunci
- Menambahkan tanda
- Membuat alias kunci
- Kunci penjadwalan untuk penghapusan

Untuk informasi selengkapnya, lihat kunci terkelola pelanggan di Panduan Pengembang AWS Key Management Service.

Tabel berikut merangkum bagaimana Amazon WorkSpaces Thin Client mengenkripsi data yang dapat diidentifikasi secara pribadi.

Jenis data	Enkripsi kunci yang dimiliki AWS	Enkripsi kunci yang dikelola pelanggan (Opsional)
Nama Lingkungan WorkSpaces Nama Lingkungan Klien Tipis	Diaktifkan	Diaktifkan
Nama perangkat WorkSpaces Nama Perangkat Klien Tipis	Diaktifkan	Diaktifkan

> **Note**
>
> Amazon WorkSpaces Thin Client secara otomatis mengaktifkan enkripsi saat istirahat dengan menggunakan kunci yang AWS dimiliki untuk melindungi data yang dapat diidentifikasi secara pribadi tanpa biaya.
> Namun, biaya AWS KMS berlaku untuk menggunakan kunci yang dikelola pelanggan. Untuk informasi selengkapnya tentang harga, lihat harga AWS Key Management Service.

Bagaimana Amazon WorkSpaces Thin Client menggunakan hibah di AWS KMS

Amazon WorkSpaces Thin Client memerlukan hibah bagi Anda untuk menggunakan kunci yang dikelola pelanggan Anda.

Saat Anda membuat Lingkungan Klien WorkSpaces Tipis yang dienkripsi dengan kunci yang dikelola pelanggan, Amazon WorkSpaces Thin Client membuat hibah atas nama Anda dengan mengirimkan CreateGrant permintaan ke AWS KMS. Hibah di AWS KMS digunakan untuk memberikan Amazon WorkSpaces Thin Client akses ke kunci KMS di akun pelanggan.

Ketika Perangkat Klien Tipis baru terdaftar ke Lingkungan terenkripsi Klien WorkSpaces Tipis dengan kunci yang dikelola pelanggan, dan nama perangkat tersebut diubah, Amazon WorkSpaces Thin Client membuat hibah atas nama Anda dengan mengirimkan CreateGrant permintaan ke AWS KMS. Hibah di AWS KMS digunakan untuk memberikan Amazon WorkSpaces Thin Client akses ke kunci KMS di akun pelanggan.

Amazon WorkSpaces Thin Client memerlukan hibah untuk menggunakan kunci terkelola pelanggan Anda untuk operasi internal berikut:

- Kirim permintaan Dekripsi ke AWS KMS untuk mendekripsi data terenkripsi

Anda dapat mencabut akses ke hibah, atau Anda dapat menghapus akses layanan ke kunci yang dikelola pelanggan kapan saja. Jika Anda melakukannya, Amazon WorkSpaces Thin Client tidak akan dapat mengakses data apa pun yang dienkripsi oleh kunci yang dikelola pelanggan, yang memengaruhi operasi yang bergantung pada data tersebut. Misalnya, jika Anda mencoba mendapatkan detail lingkungan yang tidak dapat diakses oleh Amazon WorkSpaces Thin Client, maka operasi akan mengembalikan `AccessDeniedException` kesalahan. Selain itu, perangkat WorkSpaces Thin Client tidak akan dapat menggunakan Lingkungan Klien WorkSpaces Tipis.

Buat kunci terkelola pelanggan

Anda dapat membuat kunci terkelola pelanggan simetris dengan menggunakan AWS Management Console atau operasi AWS KMS API.

Untuk membuat kunci terkelola pelanggan simetris

Ikuti langkah-langkah untuk Membuat kunci terkelola pelanggan simetris di Panduan Pengembang Layanan Manajemen AWS Kunci.

Kebijakan kunci

Kebijakan utama mengontrol akses ke kunci yang dikelola pelanggan Anda. Setiap kunci yang dikelola pelanggan harus memiliki persis satu kebijakan utama, yang berisi pernyataan yang menentukan siapa yang dapat menggunakan kunci dan bagaimana mereka dapat menggunakannya. Saat membuat kunci terkelola pelanggan, Anda dapat menentukan kebijakan kunci. Untuk informasi

selengkapnya, lihat Mengelola akses ke kunci terkelola pelanggan di Panduan Pengembang Layanan Manajemen AWS Kunci.

Untuk menggunakan kunci terkelola pelanggan Anda dengan sumber daya Amazon WorkSpaces Thin Client Anda, operasi API berikut harus diizinkan dalam kebijakan kunci:

- `kms:DescribeKey`— Memberikan detail kunci yang dikelola pelanggan sehingga Amazon WorkSpaces Thin Client dapat memvalidasi kuncinya.
- `kms:GenerateDataKey`— Memungkinkan menggunakan kunci yang dikelola pelanggan untuk mengenkripsi data.
- `kms:Decrypt`— Memungkinkan menggunakan kunci yang dikelola pelanggan untuk mendekripsi data.
- `kms:CreateGrant`— Menambahkan hibah ke kunci yang dikelola pelanggan. Memberikan akses kontrol ke kunci KMS tertentu, yang memungkinkan akses ke operasi hibah yang dibutuhkan Amazon WorkSpaces Thin Client. Untuk informasi selengkapnya tentang Menggunakan Hibah, lihat Panduan Pengembang Layanan Manajemen AWS Utama.

  Ini memungkinkan Amazon WorkSpaces Thin Client untuk melakukan hal berikut:

  - Panggilan `Decrypt` untuk mendekripsi data terenkripsi.

Berikut ini adalah contoh pernyataan kebijakan yang dapat Anda tambahkan untuk Amazon WorkSpaces Thin Client:

```
{
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi selengkapnya tentang menentukan izin dalam kebijakan, lihat Panduan Pengembang Layanan Manajemen AWS Kunci.

Untuk informasi selengkapnya tentang akses kunci pemecahan masalah, lihat Panduan Pengembang Layanan Manajemen AWS Kunci.

Menentukan kunci yang dikelola pelanggan untuk WorkSpaces Thin Client

Anda dapat menentukan kunci yang dikelola pelanggan sebagai enkripsi lapisan kedua untuk sumber daya berikut:

- WorkSpaces Lingkungan Klien Tipis

Saat membuat Lingkungan, Anda dapat menentukan kunci data dengan menyediakan`kmsKeyArn`, yang digunakan Amazon WorkSpaces Thin Client untuk mengenkripsi data pribadi yang dapat diidentifikasi.

- `kmsKeyArn`— Pengidentifikasi kunci untuk kunci yang dikelola pelanggan AWS KMS. Berikan ARN kunci.

Ketika perangkat WorkSpaces Thin Client baru ditambahkan ke Lingkungan Klien WorkSpaces Tipis yang dienkripsi dengan kunci yang dikelola pelanggan, Perangkat Klien WorkSpaces Tipis mewarisi pengaturan kunci yang dikelola pelanggan dari Lingkungan Klien WorkSpaces Tipis.

Konteks enkripsi adalah kumpulan opsional pasangan kunci-nilai yang berisi informasi kontekstual tambahan tentang data.

AWS KMS menggunakan konteks enkripsi sebagai data otentikasi tambahan untuk mendukung enkripsi yang diautentikasi. Saat Anda menyertakan konteks enkripsi dalam permintaan untuk mengenkripsi data, AWS KMS mengikat konteks enkripsi ke data terenkripsi. Untuk mendekripsi data, sertakan konteks enkripsi yang sama dalam permintaan.

Konteks enkripsi Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client menggunakan konteks enkripsi yang sama di semua operasi kriptografi AWS KMS, di mana kuncinya adalah `aws:thinclient:arn` dan nilainya adalah Nama Sumber Daya Amazon (ARN).

Berikut ini adalah konteks enkripsi Lingkungan:

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

Berikut ini adalah konteks enkripsi Perangkat:

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

Menggunakan konteks enkripsi untuk pemantauan

Bila Anda menggunakan kunci terkelola pelanggan simetris untuk mengenkripsi WorkSpaces Thin Client Environment dan data Perangkat, Anda juga dapat menggunakan konteks enkripsi dalam catatan audit dan log untuk mengidentifikasi bagaimana kunci yang dikelola pelanggan digunakan. Konteks enkripsi juga muncul di log yang dihasilkan oleh AWS CloudTrail atau Amazon CloudWatch Logs.

Menggunakan konteks enkripsi untuk mengontrol akses ke kunci terkelola pelanggan Anda

Anda dapat menggunakan konteks enkripsi dalam kebijakan utama dan kebijakan IAM sebagai kondisi untuk mengontrol akses ke kunci terkelola pelanggan simetris Anda. Anda juga dapat menggunakan kendala konteks enkripsi dalam hibah.

Amazon WorkSpaces Thin Client menggunakan batasan konteks enkripsi dalam hibah untuk mengontrol akses ke kunci yang dikelola pelanggan di akun atau Wilayah Anda. Batasan hibah mengharuskan operasi yang diizinkan oleh hibah menggunakan konteks enkripsi yang ditentukan.

Berikut ini adalah contoh pernyataan kebijakan kunci untuk memberikan akses ke kunci yang dikelola pelanggan untuk konteks enkripsi tertentu. Kondisi dalam pernyataan kebijakan ini mengharuskan `kms:Decrypt` panggilan memiliki batasan konteks enkripsi yang menentukan konteks enkripsi.

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

Memantau kunci enkripsi Anda untuk Amazon WorkSpaces Thin Client

Saat Anda menggunakan kunci terkelola pelanggan AWS KMS dengan sumber daya Amazon WorkSpaces Thin Client, Anda dapat menggunakan AWS CloudTrail atau Amazon CloudWatch Logs untuk melacak permintaan yang dikirimkan Amazon WorkSpaces Thin Client ke AWS KMS.

Contoh berikut adalah AWS CloudTrail peristiwa untuk`DescribeKey`,,, `CreateGrant` `GenerateDataKeyDecrypt`, `Decrypt` (menggunakan`Grant`) untuk memantau operasi KMS yang dipanggil oleh Amazon WorkSpaces Thin Client untuk mengakses data yang dienkripsi oleh kunci terkelola pelanggan Anda:

Dalam contoh berikut, Anda dapat melihat `encryptionContext` untuk Lingkungan Klien WorkSpaces Tipis. CloudTrail Peristiwa serupa direkam untuk Perangkat Klien WorkSpaces Tipis.

DescribeKey

Amazon WorkSpaces Thin Client menggunakan `DescribeKey` operasi untuk memverifikasi kunci yang dikelola pelanggan AWS KMS.

Contoh peristiwa berikut mencatat `DescribeKey` operasi:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
```

```
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CreateGrant

Amazon WorkSpaces Thin Client menggunakan `CreateGrant` operasi untuk membuat Hibah KMS, yang memungkinkan Anda untuk Mendekripsi data saat Perangkat mengaksesnya.

Contoh peristiwa berikut mencatat `CreateGrant` operasi:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
        "operations": ["Decrypt"],
        "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {"aws:thinclient:arn":
 "arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Amazon WorkSpaces Thin Client menggunakan `GenerateDataKey` operasi untuk mengenkripsi data.

Contoh peristiwa berikut mencatat `GenerateDataKey` operasi:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-03-12T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-03-12T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
```

```
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces Thin Client menggunakan `Decrypt` operasi untuk mendekripsi data.

Contoh peristiwa berikut mencatat `Decrypt` operasi:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt (using Grant)

Ketika Perangkat Klien WorkSpaces Tipis mengakses informasi Lingkungan atau Perangkat, `Decrypt` operasi digunakan, yang diizinkan melalui kunci KMS. `Grant`

Contoh peristiwa berikut mencatat `Decrypt` operasi, yang diotorisasi melalui`Grant`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```

Pelajari Selengkapnya

Sumber daya berikut memberikan informasi lebih lanjut tentang enkripsi data saat istirahat:

- Untuk informasi selengkapnya tentang konsep dasar AWS Key Management Service, lihat Panduan Pengembang Layanan Manajemen AWS Utama.
- Untuk informasi selengkapnya tentang praktik terbaik Keamanan untuk AWS Key Management Service, lihat Panduan Pengembang Layanan Manajemen AWS Kunci.

Enkripsi dalam bergerak

WorkSpaces Thin Client mengenkripsi data dalam perjalanan melalui HTTPS dan TLS 1.2. Anda dapat mengirim permintaan ke WorkSpaces Thin Client dengan menggunakan konsol atau panggilan API langsung. Data permintaan yang ditransfer dienkripsi dengan mengirimkannya melalui koneksi HTTPS atau TLS. Data permintaan dapat ditransfer dari AWS Console, AWS Command Line Interface, atau AWS SDK ke WorkSpaces Thin Client. Ini juga termasuk pembaruan perangkat lunak apa pun pada perangkat.

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

Manajemen kunci

Anda dapat menyediakan Kunci AWS KMS yang Dikelola Pelanggan Anda sendiri untuk mengenkripsi informasi pelanggan Anda. Jika Anda tidak menyediakan kunci, WorkSpaces Thin Client menggunakan Kunci yang AWS Dimiliki. Anda dapat mengatur kunci Anda dengan menggunakan AWS SDK.

Privasi lalu lintas kerja internet

Administrator dapat melihat acara sesi Klien WorkSpaces Tipis, termasuk waktu mulai dan informasi pembaruan perangkat lunak yang tertunda. Log ini dienkripsi dan dikirimkan dengan aman ke pelanggan di konsol WorkSpaces Thin Client. Informasi pengguna dan rincian lebih lanjut tentang sesi desktop streaming individu direkam oleh layanan desktop. Untuk informasi selengkapnya, lihat Memantau WorkSpaces, Memantau, dan Melaporkan untuk AppStream 2.0, atau Pencatatan akses pengguna untuk WorkSpaces Web.

Manajemen identitas dan akses untuk Amazon WorkSpaces Thin Client

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

Topik

Audiens

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

Pengguna layanan - Jika Anda menggunakan layanan WorkSpaces Thin Client untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur WorkSpaces Thin Client 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 Thin Client, lihatMemecahkan masalah identitas dan akses Amazon WorkSpaces Thin Client.

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya WorkSpaces Thin Client di perusahaan Anda, Anda mungkin memiliki akses penuh ke WorkSpaces Thin Client. Tugas Anda adalah menentukan fitur dan sumber daya WorkSpaces Thin Client 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 Thin Client, lihatBagaimana Amazon WorkSpaces Thin Client bekerja dengan IAM.

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

Mengautentikasi dengan identitas

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

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. 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 peran.

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

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan

metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

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

Akun AWS pengguna root

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

Identitas terfederasi

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

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

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

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya andalkan kredensial sementara daripada 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, kami sarankan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Rotasikan kunci akses secara rutin 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 dimaksudkan untuk dapat digunakan 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 adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara 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 mengautentikasi, identitas tersebut akan dikaitkan dengan peran dan diberi izin yang ditentukan oleh peran tersebut. Untuk informasi tentang peran-peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda perlu mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses

identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengorelasikan izin yang diatur 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, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). 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 — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna IAM atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Saat Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat permintaan FAS, lihat Teruskan sesi akses.
  - Peran layanan – Peran layanan adalah peran IAM yang diambil oleh 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 jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan dapat menggunakan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. 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 kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. 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 mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan dapat menentukan permintaan yang diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan konten dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke 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 bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

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 dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola 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. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola 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 sama 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 organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di sebuah organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. 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 dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Beberapa jenis kebijakan

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

Bagaimana Amazon WorkSpaces Thin Client bekerja dengan IAM

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

Fitur IAM yang dapat Anda gunakan dengan Amazon WorkSpaces Thin Client

Fitur IAM	WorkSpaces Dukungan Klien Tipis
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)	Ya
Kredensial sementara	Ya
Izin pengguna utama	Ya
Peran layanan	Tidak
Peran terkait layanan	Tidak

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

Kebijakan berbasis identitas untuk Thin Client 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 Thin Client WorkSpaces

Untuk melihat contoh kebijakan berbasis identitas Klien WorkSpaces Tipis, lihat. Contoh kebijakan berbasis identitas untuk Amazon Thin Client WorkSpaces

Kebijakan berbasis sumber daya dalam Thin Client 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. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, 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 prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas 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 Thin Client

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON 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 dengan operasi AWS API 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 Klien WorkSpaces Tipis, lihat Tindakan yang Ditentukan oleh Amazon WorkSpaces Thin Client di Referensi Otorisasi Layanan.

Tindakan kebijakan di WorkSpaces Thin Client menggunakan awalan berikut sebelum tindakan:

```
workspaces-thin-client
```

Untuk menentukan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma, seperti yang ditunjukkan pada contoh berikut:

```
"Action": [
      "workspaces-thin-client:action1",
      "workspaces-thin-client:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Klien WorkSpaces Tipis, lihat. Contoh kebijakan berbasis identitas untuk Amazon Thin Client WorkSpaces

Sumber daya kebijakan untuk WorkSpaces Thin Client

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON 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 Klien WorkSpaces Tipis dan ARNnya, lihat Sumber Daya yang Ditentukan oleh Amazon WorkSpaces Thin Client di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh Amazon WorkSpaces Thin Client.

Untuk melihat contoh kebijakan berbasis identitas Klien WorkSpaces Tipis, lihat. Contoh kebijakan berbasis identitas untuk Amazon Thin Client WorkSpaces

Kunci kondisi kebijakan untuk Klien WorkSpaces Tipis

Mendukung kunci kondisi kebijakan spesifik layanan	Ya

Administrator dapat menggunakan kebijakan AWS JSON 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 nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

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

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

Untuk melihat daftar kunci kondisi Klien WorkSpaces Tipis, lihat Kunci Kondisi untuk Amazon WorkSpaces Thin Client di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh Amazon WorkSpaces Thin Client.

Untuk melihat contoh kebijakan berbasis identitas Klien WorkSpaces Tipis, lihat. Contoh kebijakan berbasis identitas untuk Amazon Thin Client WorkSpaces

ACL di WorkSpaces Thin Client

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.

ABAC dengan Klien WorkSpaces Tipis

Mendukung ABAC (tanda dalam kebijakan)	Ya

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

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

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

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi 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 WorkSpaces Thin Client

Mendukung kredensial sementara	Ya

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

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. 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 kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk WorkSpaces Klien Tipis

Mendukung sesi akses maju (FAS)	Ya

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

Peran layanan untuk Klien WorkSpaces Tipis

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 mengganggu fungsionalitas Klien WorkSpaces Tipis. Edit peran layanan hanya ketika WorkSpaces Thin Client memberikan panduan untuk melakukannya.

Peran terkait layanan untuk WorkSpaces Thin Client

Mendukung peran terkait layanan	Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat menggunakan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. 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 Thin Client WorkSpaces

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Klien WorkSpaces Tipis. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka 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 Klien WorkSpaces Tipis, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Amazon WorkSpaces Thin Client dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol WorkSpaces Thin Client
- Berikan akses read-only ke Thin Client WorkSpaces
- Izinkan pengguna melihat izin mereka sendiri
- Berikan akses penuh ke WorkSpaces Thin Client

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi 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. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti 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.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk 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 Thin Client

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

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

Berikan akses read-only ke Thin Client WorkSpaces

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang memungkinkan pengguna IAM untuk melihat konfigurasi WorkSpaces Thin Client, tetapi tidak membuat perubahan. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau program dengan menggunakan AWS CLI atau AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "thinclient:GetEnvironment",
                "thinclient:ListEnvironments",
                "thinclient:GetDevice",
                "thinclient:ListDevices",
                "thinclient:ListDeviceSessions",
                "thinclient:GetSoftwareSet",
                "thinclient:ListSoftwareSets",
                "thinclient:ListTagsForResource"
            ],
```

```
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

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 ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

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

Berikan akses penuh ke WorkSpaces Thin Client

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang memberikan akses penuh ke pengguna IAM Klien WorkSpaces Tipis. Kebijakan ini mencakup izin untuk menyelesaikan semua tindakan Klien WorkSpaces Tipis di konsol atau program dengan menggunakan AWS CLI atau AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["thinclient:*"],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

Memecahkan masalah identitas dan akses Amazon WorkSpaces Thin Client

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

Topik

- Saya tidak berwenang untuk melakukan tindakan di WorkSpaces Thin Client
- Saya ingin melihat access key saya
- Saya seorang administrator dan ingin mengizinkan orang lain mengakses Klien WorkSpaces Tipis
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Klien WorkSpaces Tipis saya

Saya tidak berwenang untuk melakukan tindakan di WorkSpaces Thin Client

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator adalah orang yang memberikan nama pengguna dan kata sandi kepada Anda.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya fiktif *`my-thin-client-device`*, tetapi tidak memiliki izin fiktif `workspaces-thin-client:`*`ListDevices`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-thin-client:ListDevices on resource: my-thin-client-device
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya mengakses *`my-thin-client-device`* sumber daya dengan menggunakan `workspaces-thin-client:`*`ListDevices`* tindakan tersebut.

Saya ingin melihat access key saya

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

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

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

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

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Klien WorkSpaces Tipis

Untuk memungkinkan orang lain mengakses WorkSpaces Thin Client, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Mereka akan menggunakan kredensial untuk entitas tersebut untuk mengakses AWS. Anda kemudian harus melampirkan kebijakan ke entitas yang memberi mereka izin yang benar di WorkSpaces Thin Client.

Untuk segera mulai, lihat Membuat pengguna dan grup khusus IAM pertama Anda di Panduan Pengguna IAM.

Untuk informasi selengkapnya, lihat Berikan akses penuh ke WorkSpaces Thin Client.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Klien WorkSpaces Tipis 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 Thin Client mendukung fitur-fitur ini, lihatBagaimana Amazon WorkSpaces Thin Client bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Memberikan akses kepada pengguna eksternal yang sah (federasi 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.

Ketahanan di Amazon WorkSpaces Thin Client

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

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

Selain infrastruktur AWS global, WorkSpaces Thin Client menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Analisis dan manajemen kerentanan di Amazon WorkSpaces Thin Client

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara Anda AWS dan Anda. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Amazon WorkSpaces Thin Client terintegrasi silang dengan Amazon, WorkSpaces Amazon AppStream 2.0, dan WorkSpaces Web. Lihat tautan berikut untuk informasi selengkapnya tentang manajemen pembaruan untuk masing-masing layanan ini:

- Perbarui Manajemen di Amazon AppStream 2.0
- Perbarui manajemen di Amazon WorkSpaces
- Analisis konfigurasi dan kerentanan di Amazon Web WorkSpaces

Memantau Amazon WorkSpaces Thin Client

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon WorkSpaces Thin Client dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton WorkSpaces Thin Client, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- 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 yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Mencatat panggilan Amazon WorkSpaces Thin Client API dengan menggunakan AWS CloudTrail

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

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

WorkSpaces Informasi Klien Tipis di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di WorkSpaces Thin Client, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh

peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

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

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

Semua tindakan WorkSpaces Thin Client dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API Amazon WorkSpaces Thin Client. Misalnya, panggilan ke`CreateEnvironment`,`ListDevices`, dan `GetSoftwareSet` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log Klien WorkSpaces Tipis

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili

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

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "arn:aws:iam::<arn>",
                "accountId": "<accpimt-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-18T23:07:01Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-18T23:11:57Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "GetDevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<source-ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
 Gecko/20100101 Firefox/115.0",
    "requestParameters": {
        "id": "<ip>"
    },
    "responseElements": null,
    "requestID": "<request-id>",
    "eventID": "<event-id>",
```

```
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<recipient-account-id>",
    "eventCategory": "Management"
}
```

Membuat sumber daya Amazon WorkSpaces Thin Client dengan AWS CloudFormation

Amazon WorkSpaces Thin Client terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya Anda. Dengan cara ini, Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti Lingkungan), dan AWS CloudFormation ketentuan serta mengonfigurasi sumber daya tersebut untuk Anda.

Bila Anda menggunakan AWS CloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur sumber daya WorkSpaces Thin Client Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang kali di beberapa Akun AWS dan Wilayah.

WorkSpaces Klien Tipis dan AWS CloudFormation template

Untuk menyediakan dan mengonfigurasi sumber daya untuk WorkSpaces Thin Client dan layanan terkait, Anda harus memahami AWS CloudFormation template. Template adalah file teks yang diformat dalam format JSON atau YAMAL. Template ini menjelaskan sumber daya yang ingin Anda sediakan di AWS CloudFormation tumpukan Anda. Jika Anda tidak terbiasa dengan format JSON atau YAMAL, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan template. AWS CloudFormation Untuk informasi selengkapnya, lihat Apa itu AWS CloudFormation Designer? di Panduan Pengguna AWS CloudFormation .

WorkSpaces Thin Client mendukung pembuatan Lingkungan di AWS CloudFormation. Untuk informasi selengkapnya, termasuk contoh templat JSON dan YAMAL untuk Lingkungan, lihat referensi jenis sumber daya Amazon WorkSpaces Thin Client di AWS CloudFormation Panduan Pengguna.

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormation Panduan Pengguna

- Referensi AWS CloudFormation API
- AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah

Akses Amazon WorkSpaces Thin Client dengan menggunakan endpoint antarmuka ()AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan Amazon WorkSpaces Thin Client. Anda dapat mengakses WorkSpaces Thin Client sebagai VPC, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk WorkSpaces mengakses Thin Client.

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka yang didukung oleh AWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan untuk Thin Client. WorkSpaces

Untuk informasi selengkapnya, lihat Mengakses Layanan AWS melalui AWS PrivateLink di Panduan AWS PrivateLink .

Pertimbangan untuk WorkSpaces Thin Client

Sebelum Anda menyiapkan titik akhir antarmuka untuk WorkSpaces Thin Client, tinjau Pertimbangan dalam Panduan.AWS PrivateLink

WorkSpaces Thin Client mendukung panggilan ke semua tindakan API-nya melalui titik akhir antarmuka.

Buat titik akhir antarmuka untuk WorkSpaces Thin Client

Anda dapat membuat titik akhir antarmuka untuk WorkSpaces Thin Client dengan menggunakan konsol VPC Amazon atau AWS Command Line Interface ().AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat endpoint antarmuka untuk WorkSpaces Thin Client dengan menggunakan nama layanan berikut:

```
com.amazonaws.region.thinclient.api
```

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API ke WorkSpaces Thin Client dengan menggunakan nama DNS Regional default. Misalnya, `api.thinclient.us-east-1.amazonaws.com`.

Buat kebijakan titik akhir untuk titik akhir antarmuka Anda

Kebijakan endpoint adalah sumber daya IAM yang dapat Anda lampirkan ke titik akhir antarmuka. Kebijakan endpoint default memberi Anda akses penuh ke WorkSpaces Thin Client melalui titik akhir antarmuka. Untuk mengontrol akses yang diberikan ke WorkSpaces Thin Client dari VPC Anda, lampirkan kebijakan endpoint khusus ke titik akhir antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal yang dapat melakukan tindakan (Akun AWS, pengguna IAM, dan peran IAM).
- Tindakan yang dapat dilakukan.
- Sumber daya untuk melakukan tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan menggunakan kebijakan titik akhir di Panduan AWS PrivateLink .

Contoh: Kebijakan titik akhir VPC untuk WorkSpaces tindakan Klien Tipis

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka Anda, kebijakan ini memberikan akses ke tindakan Klien WorkSpaces Tipis yang terdaftar untuk semua prinsip di semua sumber daya.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "thinclient:ListEnvironments",
            "thinclient:ListDevices",
            "thinclient:ListSoftwareSets"
         ],
         "Resource":"*"
      }
   ]
```

```
}
```

Riwayat dokumen untuk Panduan Administrator Klien WorkSpaces Tipis

Tabel berikut menjelaskan riwayat dokumentasi untuk rilis Panduan Administrator Klien WorkSpaces Tipis.

Perubahan	Deskripsi	Tanggal
• Mengkonfigurasi WorkSpaces untuk Amazon WorkSpaces Thin Client • Mengkonfigurasi AppStream 2.0 untuk Amazon WorkSpaces Thin Client	• Memperbarui daftar sistem operasi. • Memperbarui prosedur Penyedia Identitas.	Februari 12, 2024
Rilis awal	Rilis awal	26 November 2023

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