



Panduan Administrator

Klien WorkSpaces Tipis Amazon



Klien WorkSpaces Tipis Amazon: Panduan Administrator

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Apa itu konsol administrator Amazon WorkSpaces Thin Client?	1
Apakah Anda pengguna baru?	1
Arsitektur	1
Menyiapkan konsol administrator Amazon WorkSpaces Thin Client	4
Daftar AWS	4
Mmebuat pengguna IAM	4
Memulai dengan konsol administrator VDI untuk Amazon WorkSpaces Thin Client	6
Mengkonfigurasi WorkSpaces Pribadi untuk Klien WorkSpaces Tipis	6
Sebelum Anda mulai	7
Langkah 1: Verifikasi bahwa sistem Anda memenuhi fitur yang diperlukan WorkSpaces Pribadi	7
Langkah 2: Gunakan pengaturan lanjutan untuk meluncurkan Workspace	8
Kelanjutan bisnis	9
Mengkonfigurasi WorkSpaces Kolam untuk Klien WorkSpaces Tipis	10
Sebelum Anda mulai	10
Buat WorkSpaces Pool	10
Mengkonfigurasi akses Klien WorkSpaces Tipis	13
Mengkonfigurasi WorkSpaces Aplikasi untuk Amazon WorkSpaces Thin Client	14
Langkah 1: Verifikasi bahwa sistem Anda memenuhi fitur yang diperlukan WorkSpaces Aplikasi	14
Langkah 2: Siapkan tumpukan WorkSpaces Aplikasi Anda	15
Mengkonfigurasi Amazon WorkSpaces Secure Browser untuk Amazon WorkSpaces Thin Client	16
Langkah 1: Verifikasi bahwa sistem Anda memenuhi fitur yang diperlukan Amazon WorkSpaces Secure Browser	16
Langkah 2: Siapkan portal Browser WorkSpaces Aman	17
Memulai konsol administrator Klien WorkSpaces Tipis	18
Daerah tertutup	18
Meluncurkan konsol administrator WorkSpaces Thin Client	19
Menggunakan konsol administrator WorkSpaces Thin Client	20
Lingkungan	21
Daftar lingkungan	21
Detail Lingkungan	23
Pembuatan lingkungan	26

Mengedit lingkungan	30
Menghapus lingkungan	31
Perangkat	31
Daftar perangkat	31
Detail perangkat	34
Mengedit nama perangkat	41
Menyetel ulang dan membatalkan pendaftaran perangkat	41
Mengarsipkan perangkat	42
Menghapus perangkat	42
Mengekspor detail perangkat	43
Pembaruan perangkat lunak	44
Memperbarui perangkat lunak lingkungan	45
Memperbarui perangkat lunak perangkat	46
WorkSpaces Rilis perangkat lunak Thin Client	46
Menggunakan tag pada sumber daya WorkSpaces Thin Client	59
Keamanan	62
Perlindungan data	62
Enkripsi data	64
Enkripsi saat diam	65
Enkripsi saat bergerak	79
Manajemen kunci	79
Privasi lalu lintas kerja internet	80
Manajemen identitas dan akses	80
Audiens	80
Mengautentikasi dengan identitas	81
Mengelola akses menggunakan kebijakan	82
Bagaimana Amazon WorkSpaces Thin Client bekerja dengan IAM	84
Contoh kebijakan berbasis identitas	90
AWS kebijakan terkelola	95
Pemecahan masalah	101
Ketahanan	104
Analisis dan Manajemen Kerentanan	104
Pemantauan	105
CloudTrail log	105
CloudTrail peristiwa data	107
CloudTrail acara manajemen	108

CloudTrail contoh acara	108
Pantau menggunakan CloudWatch metrik	111
WorkSpaces Metrik Klien Tipis	112
AWS CloudFormation sumber daya	115
WorkSpaces Klien Tipis dan CloudFormation template	115
Pelajari lebih lanjut tentang CloudFormation	115
AWS PrivateLink	117
Pertimbangan	117
Membuat sebuah titik akhir antarmuka	117
Membuat kebijakan titik akhir	118
Riwayat dokumen	119
.....	cxxii

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?](#)
- [Arsitektur](#)

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](#)
- [WorkSpaces Aplikasi](#)
- [Browser WorkSpaces Aman Amazon](#)

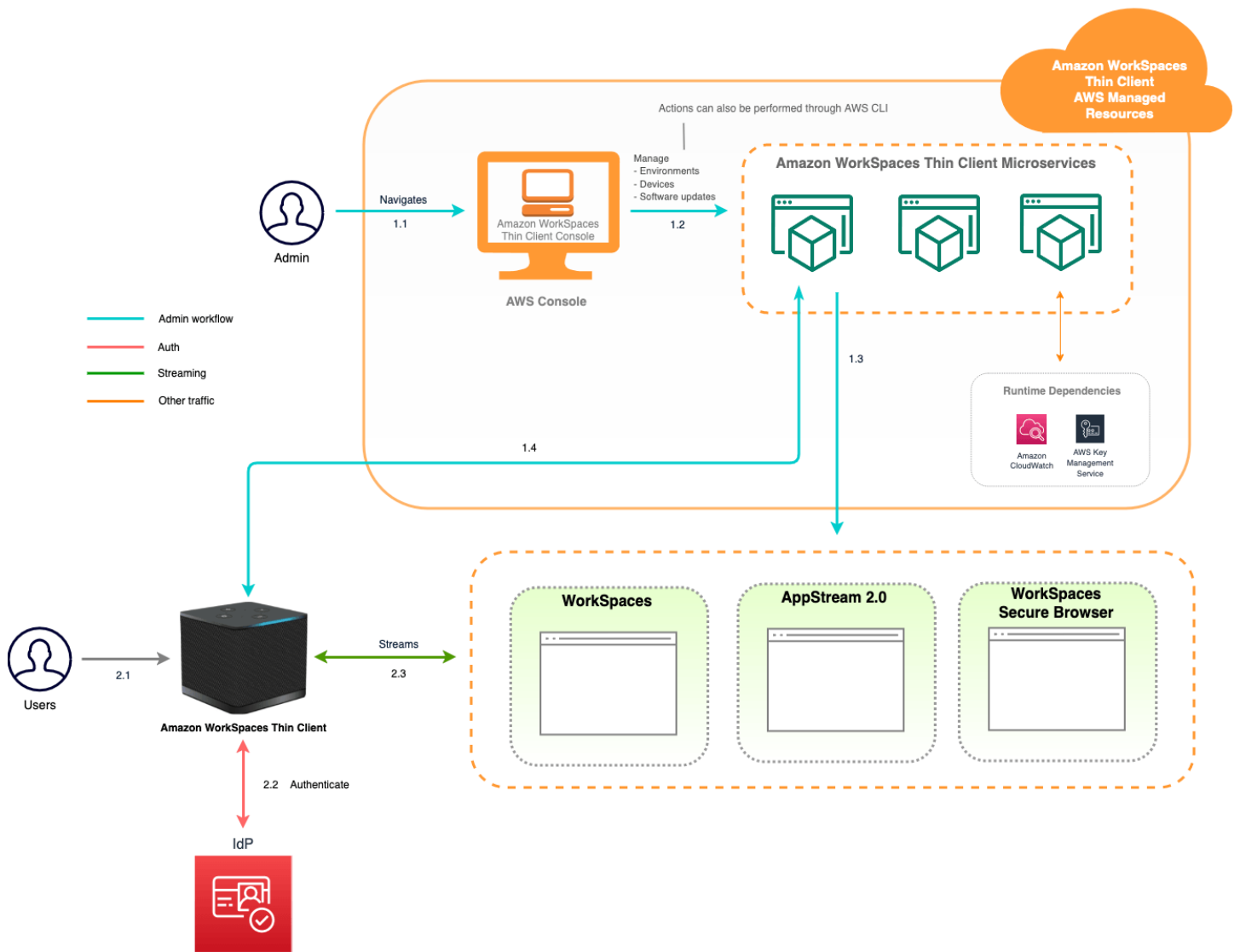
Bergantung pada VDI yang digunakan, informasi untuk Klien WorkSpaces Tipis Anda diakses dan dikelola baik melalui direktori untuk WorkSpaces, tumpukan untuk WorkSpaces Aplikasi, dan titik akhir portal web untuk Browser Aman. WorkSpaces

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

Untuk informasi selengkapnya tentang WorkSpaces Aplikasi, lihat [Memulai WorkSpaces Aplikasi Amazon: Mengatur Dengan Contoh Aplikasi](#). WorkSpaces Aplikasi mengelola AWS sumber daya yang diperlukan untuk meng-host dan menjalankan aplikasi Anda, menskalakan secara otomatis, dan menyediakan akses ke pengguna sesuai permintaan. WorkSpaces Aplikasi 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-serviceSaaS). 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.



Menyiapkan konsol administrator Amazon WorkSpaces Thin Client

Topik

- [Daftar AWS](#)
- [Mmebuat pengguna IAM](#)

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/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. 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.	Konfigurasi 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 di Buat pengguna IAM untuk akses darurat di Panduan Pengguna IAM.	Konfigurasi 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 konfigurasi 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 Pribadi untuk Klien WorkSpaces Tipis](#)
- [Mengkonfigurasi WorkSpaces Kolam untuk Klien WorkSpaces Tipis](#)
- [Mengkonfigurasi WorkSpaces Aplikasi untuk Amazon WorkSpaces Thin Client](#)
- [Mengkonfigurasi Amazon WorkSpaces Secure Browser untuk Amazon WorkSpaces Thin Client](#)

Mengkonfigurasi WorkSpaces Pribadi untuk Klien WorkSpaces Tipis

Agar WorkSpaces Thin Client dapat digunakan dengan Amazon WorkSpaces Personal, layanan Anda perlu dikonfigurasi untuk mengakses WorkSpaces direktori. Direktori Amazon WorkSpaces Personal 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](#) Personal.
- 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 Pribadi](#).
- Saat Anda meluncurkan WorkSpace, aktifkan dan konfigurasi akses web WorkSpaces Thin Client. Untuk informasi selengkapnya, lihat [Mengonfigurasi Klien WorkSpaces Tipis](#)

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

Agar konsol administrator Klien WorkSpaces Tipis berfungsi dengan baik dengan Amazon WorkSpaces Personal, 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 DCV

Langkah 2: Gunakan pengaturan lanjutan untuk meluncurkan Workspace

Untuk menggunakan pengaturan lanjutan untuk meluncurkan Workspace

1. Buka WorkSpaces konsol di <https://console.aws.amazon.com/workspaces/v2/home/>.
2. Pilih salah satu jenis direktori berikut, lalu pilih Berikutnya:
 - AWS Microsoft AD yang dikelola
 - 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.

Kelanjutan bisnis

WorkSpaces Thin Client memberikan dukungan untuk kelangsungan Bisnis sebagai bagian dari [Business Continuity Plan \(BCP\)](#). WorkSpaces Kontinuitas bisnis Thin Client tersedia untuk digunakan hanya dengan WorkSpaces Pribadi. Untuk informasi selengkapnya tentang kelangsungan bisnis, lihat [Kelangsungan bisnis untuk WorkSpaces Pribadi](#) di panduan WorkSpaces Administrasi Amazon.

Prasyarat

Agar kelangsungan bisnis bekerja pada WorkSpaces Thin Client, prasyarat berikut harus dipenuhi:

- Untuk Pengalihan WorkSpaces Lintas Wilayah — Layanan DNS dan kebijakan perutean telah dikonfigurasi. Untuk mengaturnya, lihat [Mengonfigurasi layanan DNS Anda dan mengatur kebijakan perutean DNS](#).
- Untuk Ketahanan WorkSpaces Multi-Wilayah - Siaga telah dibuat WorkSpaces . Untuk membuat ini, lihat [Membuat siaga Workspace](#).
- Alias koneksi di wilayah menggunakan WorkSpaces Thin Client. Untuk memverifikasi wilayah Anda, lihat [Wilayah yang dicakup](#).

Mengkonfigurasi kelangsungan bisnis untuk WorkSpaces Thin Client

Untuk mengaktifkan DR WorkSpaces Pribadi di Amazon WorkSpaces Thin Client, Anda perlu mengonfigurasi alias koneksi untuk memetakan ke lingkungan menggunakan SDK.

Contoh penjelasan dokumen untuk menyiapkan pemulihan bencana:

Example

Contoh perintah menggunakan AWS CLI untuk membuat lingkungan baru menggunakan alias WorkSpaces koneksi untuk desktop streaming:

```
aws workspaces-thin-client create-environment --region region --desktop-arn/  
arn:aws:workspaces:region:account:connectionalias/wsca-id
```

Ganti *wsca-id* dengan alias koneksi WorkSpaces Pribadi Anda. ID alias WorkSpaces koneksi dapat ditemukan di WorkSpaces Management Console atau dari SDK.

Pengalaman pengguna akhir

Setelah kelangsungan bisnis dikonfigurasi, perangkat harus terdaftar dan aktif dalam 15 hari terakhir. Setelah itu, jika layanan manajemen Klien WorkSpaces Tipis menjadi tidak tersedia, pengguna kemudian dapat tetap terhubung ke sesi mereka hingga 24 jam. Dalam kondisi ini, perangkat tidak akan menerima pembaruan perangkat lunak, bertukar informasi postur, dan tidak dapat diaktifkan. Entri perangkat yang sesuai di konsol Klien WorkSpaces Tipis tidak akan menampilkan informasi terbaru.

Jika layanan manajemen perangkat Klien WorkSpaces Tipis tetap tidak tersedia setelah 24 jam, pesan kesalahan berikut akan ditampilkan:

“Telah terjadi kesalahan. Coba lagi. Jika masalah berlanjut, hubungi administrator TI Anda. (Kode Kesalahan: 3006).”

Mengkonfigurasi WorkSpaces Kolam untuk Klien WorkSpaces Tipis

Agar WorkSpaces Thin Client dapat digunakan dengan Amazon WorkSpaces Pools, penyedia identitas SAMP 2.0 (iDP) Anda perlu dikonfigurasi untuk mengakses WorkSpaces direktori Pools. Direktori Amazon WorkSpaces Pools adalah kumpulan non-persisten yang WorkSpaces ditugaskan ke sekelompok pengguna.

Note

Konfigurasi harus dilakukan sebelum menggunakan konsol untuk pertama kalinya.

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 yang tercantum di [Sebelum Anda Mulai Menggunakan Direktori Aktif dengan WorkSpaces Kumpulan](#) di Panduan WorkSpaces Administrasi Amazon sebelum Anda melanjutkan konfigurasi Anda.

Buat WorkSpaces Pool

Siapkan dan buat kumpulan tempat aplikasi pengguna diluncurkan dan dialirkan.

Note

Anda harus membuat direktori sebelum membuat WorkSpaces Pool. Untuk informasi selengkapnya, lihat [Mengkonfigurasi SAMP 2.0 dan membuat direktori direktori WorkSpaces Pools](#).

Untuk mengatur dan membuat kolam

1. Buka WorkSpaces konsol di <https://console.aws.amazon.com/workspaces/v2/home/>.
2. Di panel navigasi, pilih WorkSpaces, Pools.
3. Pilih Buat WorkSpaces Kolam.
4. Di bawah Onboarding (opsional), Anda dapat memilih opsi Rekomendasikan kepada saya berdasarkan kasus penggunaan saya untuk mendapatkan rekomendasi tentang jenis yang ingin WorkSpaces Anda gunakan. Anda dapat melewati langkah ini jika Anda tahu bahwa Anda ingin menggunakan WorkSpaces Pools.
5. Di bawah Konfigurasi WorkSpaces, masukkan detail berikut:
 - Untuk Nama, masukkan pengenalan nama unik untuk kumpulan. Karakter khusus tidak diperbolehkan.
 - Untuk Deskripsi, masukkan deskripsi untuk kumpulan (maksimal 256 karakter).
 - Untuk Bundle, pilih dari jenis bundel berikut yang ingin Anda gunakan untuk Anda WorkSpaces.
 - Gunakan WorkSpaces bundel dasar - Pilih salah satu bundel dari drop down. Untuk informasi selengkapnya tentang jenis bundel yang Anda pilih, pilih Detail bundel. Untuk membandingkan bundel yang ditawarkan untuk pool, pilih Bandingkan semua bundel.
 - Gunakan bundel kustom Anda sendiri — Pilih bundel yang sebelumnya Anda buat. Untuk membuat bundel kustom, lihat [Membuat WorkSpaces gambar kustom dan bundel untuk WorkSpaces Pribadi](#).

Note

BYOL saat ini tidak tersedia untuk WorkSpaces Pools.

- Untuk Durasi sesi maksimum dalam hitungan menit, pilih jumlah waktu maksimum yang sesi streaming dapat tetap aktif. Jika pengguna masih terhubung ke instans streaming lima menit

sebelum batas ini tercapai, mereka akan diminta untuk menyimpan dokumen yang terbuka sebelum terputus. Setelah waktu ini berlalu, instans dihentikan dan diganti dengan instans baru. Durasi sesi maksimum yang dapat Anda atur di konsol WorkSpaces Pools adalah 5760 menit (96 jam). Durasi sesi maksimum yang dapat Anda atur menggunakan WorkSpaces Pools API dan CLI adalah 432000 detik (120 jam).

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

Note

Pengguna dianggap dalam keadaan diam ketika mereka berhenti memberikan input keyboard atau mouse selama sesi streaming mereka. Untuk kumpulan yang bergabung dengan domain, hitungan mundur untuk batas waktu pemutusan idle tidak dimulai sampai pengguna masuk dengan kata sandi domain Direktori Aktif mereka atau dengan kartu pintar. Unggahan dan unduhan file, audio masuk, audio keluar, dan perubahan piksel tidak memenuhi syarat sebagai aktivitas pengguna. Jika pengguna terus menganggur setelah interval waktu di batas waktu pemutusan Idle dalam beberapa menit berlalu, mereka terputus.

- Untuk kebijakan kapasitas terjadwal (opsional), pilih Tambahkan kapasitas jadwal baru. Tunjukkan tanggal dan waktu mulai dan berakhir kapan harus menyediakan jumlah instans

minimum dan maksimum untuk kumpulan Anda berdasarkan jumlah minimum pengguna bersamaan yang diharapkan.

- Untuk kebijakan penskalaan Manual (opsional), tentukan kebijakan penskalaan untuk kumpulan yang akan digunakan untuk menambah dan mengurangi kapasitas kumpulan Anda. Perluas kebijakan penskalaan Manual untuk menambahkan kebijakan penskalaan baru.

 Note

Ukuran kolam Anda dibatasi oleh kapasitas minimum dan maksimum yang Anda tentukan.

- Pilih Tambahkan kebijakan skala baru dan masukkan nilai untuk menambahkan instance tertentu jika pemanfaatan kapasitas yang ditentukan kurang atau lebih dari nilai ambang batas yang ditentukan.
 - Pilih Tambahkan skala baru dalam kebijakan dan masukkan nilai untuk menghapus instance tertentu jika pemanfaatan kapasitas yang ditentukan kurang atau lebih dari nilai ambang batas yang ditentukan.
 - Untuk Tag, tentukan nilai key pair yang ingin Anda gunakan. Kunci dapat berupa kategori umum, seperti "proyek," "pemilik," atau "lingkungan," dengan nilai terkait tertentu.
6. Pada halaman Pilih direktori, pilih direktori yang Anda buat. Untuk membuat direktori, pilih Buat direktori. Untuk informasi selengkapnya, lihat [Mengelola direktori untuk WorkSpaces Kumpulan](#).
 7. Pilih Buat WorkSpace Kolam.

Mengkonfigurasi akses Klien WorkSpaces Tipis

Mengkonfigurasi akses web untuk WorkSpaces Pools untuk menggunakan WorkSpaces Thin Client, Anda harus menggunakan antarmuka tanah AWS perintah.

1. Instal atau perbarui [AWS Command Line Interface](#).
2. Konfigurasi [AWS CLI pengaturan](#) Anda.
3. Buka AWS CLI.
4. Jalankan penggantian berikut WORKSPACES_DIRECTORY_ID dan REGION dengan informasi yang sesuai:

```
aws workspaces modify-workspace-access-properties --resource-id WORKSPACES_DIRECTORY_ID --workspace-access-properties '{"DeviceTypeWorkSpacesThinClient":"ALLOW"}' --region REGION
```

Mengkonfigurasi WorkSpaces Aplikasi untuk Amazon WorkSpaces Thin Client

WorkSpaces Instans aplikasi akan terdaftar berdasarkan nama Stack dan akan memerlukan URL login iDP untuk dikonfigurasi pada halaman buat lingkungan. Karena otentikasi SAMP untuk WorkSpaces Aplikasi 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 fitur yang diperlukan WorkSpaces Aplikasi

Agar konsol administrator WorkSpaces Thin Client berfungsi dengan WorkSpaces Aplikasi 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 WorkSpaces Aplikasi untuk membuat Penyedia Identitas. Saat diminta untuk Buat konsol env, masukkan URL Login IDP Anda.
Sistem operasi	Windows

Fitur	Persyaratan
Jenis Platform	Windows Server (2012 R2, 2016 atau 2019)
Papan klip	Nonaktifkan Dikonfigurasi pada tingkat tumpukan WorkSpaces Aplikasi
Transfer file	Nonaktifkan Dikonfigurasi pada tingkat tumpukan WorkSpaces Aplikasi
Mencetak ke perangkat lokal	Nonaktifkan Dikonfigurasi pada tingkat tumpukan WorkSpaces Aplikasi

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

Langkah 2: Siapkan tumpukan WorkSpaces Aplikasi Anda

Untuk melakukan streaming aplikasi Anda, WorkSpaces Aplikasi 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 WorkSpaces Aplikasi: 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, konfigurasi 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
Papan klip	Nonaktifkan
Transfer file	Nonaktifkan
Mencetak ke perangkat 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

- [Daerah tertutup](#)
- [Meluncurkan konsol administrator WorkSpaces Thin Client](#)

Daerah tertutup

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
Europa (Irlandia)	eu-west-1	thinclient.eu-west-1.amazonaws.com	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
Europa (Frankfurt)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europa (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

End User Computing

Amazon WorkSpaces Thin Client

Affordable, easy-to-manage thin client for secure access to virtual desktops

Improve end-user productivity by going from unboxing to desktop access in just a few minutes, while improving IT staff productivity through centralized remote management of your fleet.

Amazon WorkSpaces Thin Client

Create WorkSpaces Thin Client environment, enabling users to securely access virtual desktops.

[Get started](#) [Order devices](#)

How it works

Admin management flow

```
graph LR; A[Amazon WorkSpaces Thin Client  
Cost-effective, secure, and easy-to-manage access to virtual desktops] --> B[Administrator sets up Amazon WorkSpaces, Amazon WorkSpaces Web, or Amazon AppStream 2.0 in desired AWS Region to associate with WorkSpaces Thin Client service]; B --> C[Administrator copies activation codes from Console and emails them to end users]; C --> D[End users enter activation code to register the device and log into their virtual desktop environment]; D --> E[Administrator manages, monitors, and maintains WorkSpaces Thin Client fleet and controls access through device management service];
```

Amazon WorkSpaces Thin Client
Cost-effective, secure, and easy-to-manage access to virtual desktops

Administrator sets up Amazon WorkSpaces, Amazon WorkSpaces Web, or Amazon AppStream 2.0 in desired AWS Region to associate with WorkSpaces Thin Client service

Administrator copies activation codes from Console and emails them to end users

End users enter activation code to register the device and log into their virtual desktop environment

Administrator manages, monitors, and maintains WorkSpaces Thin Client fleet and controls access through device management service

Pricing

You pay up front for the WorkSpaces Thin Client device, plus a monthly service fee per device to manage, monitor, and maintain your thin client fleet in the WorkSpaces Thin Client management console.

[Learn more about WorkSpaces Thin Client pricing](#)

Amazon WorkSpaces Thin Client devices

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](#)
- [Perangkat](#)
- [Pembaruan perangkat lunak](#)

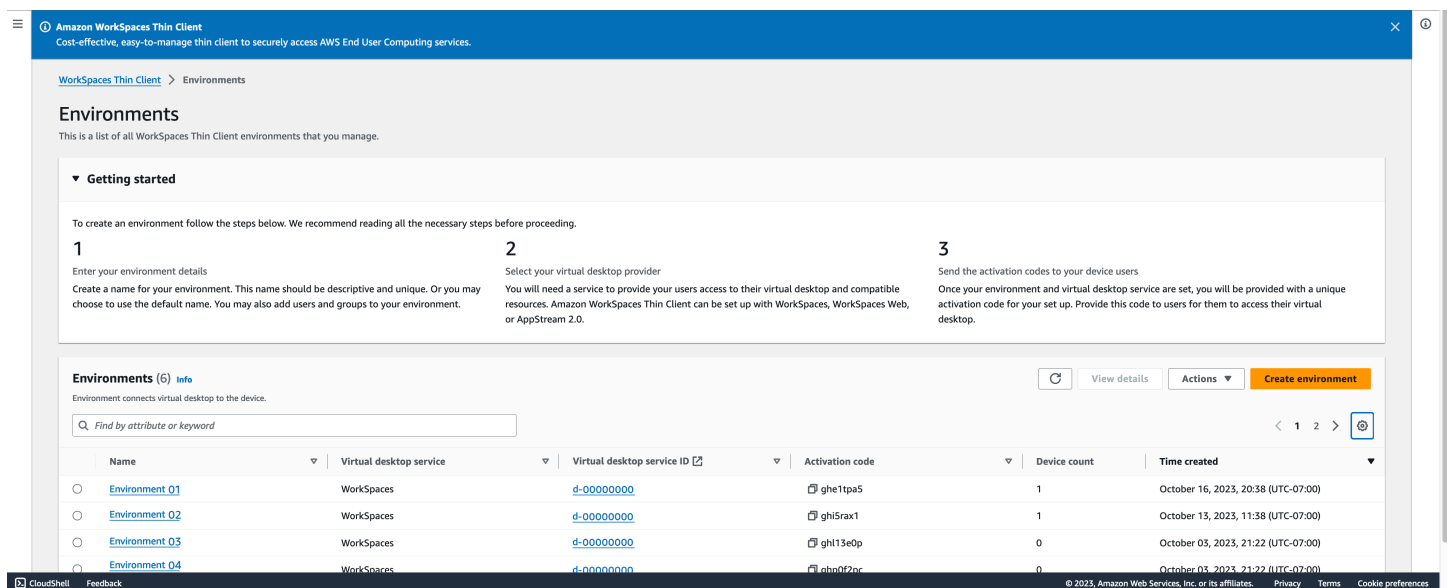
Lingkungan

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](#)
- [WorkSpaces Aplikasi](#)
- [Browser WorkSpaces Aman Amazon](#)

Daftar lingkungan

Ada sejumlah parameter untuk lingkungan Anda untuk Anda tinjau serta beberapa tindakan yang dapat Anda ambil.



Rincian daftar lingkungan

Parameter untuk lingkungan Anda tercantum untuk ulasan Anda. Tabel berikut mencantumkan setiap elemen dalam ringkasan dan bagaimana fungsinya.

Elemen	Deskripsi
Nama	Pengidentifikasi unik yang terkait dengan lingkungan ini.

Elemen	Deskripsi
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.
Waktu Dibuat	Tanggal dan waktu lingkungan diciptakan.

Tindakan daftar lingkungan

Ada sejumlah tindakan yang dapat Anda lakukan dari sini. Pilih salah satu dari ini untuk melakukan tindakan yang sesuai.

Elemen	Deskripsi
Pencarian	Mencari semua lingkungan yang Anda kelola.
Refresh	Menyegarkan daftar lingkungan.
Lihat detail	Menampilkan detail Lingkungan .
Tindakan	Membuka daftar tarik-turun tempat Anda dapat Mengedit atau Menghapus lingkungan.
Ciptakan lingkungan	Memulai proses menciptakan lingkungan .

Topik

- [Detail Lingkungan](#)
- [Pembuatan lingkungan](#)

- [Mengedit lingkungan](#)
- [Menghapus lingkungan](#)

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](#)
- [Detail lingkungan desktop virtual](#)

Ringkasan

Bagian Ringkasan memberikan ikhtisar tingkat tinggi tentang fitur-fitur utama dari Lingkungan Klien WorkSpaces Tipis. Tabel berikut mencantumkan setiap elemen dalam ringkasan dan bagaimana fungsinya.

Summary		
Name DRK Environment - Mon, Aug 7, 2023, 16:03:41	Always keep software up-to-date Yes	Activation code
Virtual desktop service WorkSpaces Web	Maintenance window start time 00:00 (Device local time)	Associated devices 1
Virtual desktop service ID	Maintenance window end time 03:00 (Device local time)	Time created August 07, 2023, 16:04 (UTC-04:00)
	Maintenance window days of the week Sunday	Time last modified August 07, 2023, 16:04 (UTC-04:00)

Elemen	Deskripsi
Nama	Pengidentifikasi unik yang terkait dengan lingkungan ini.
Layanan desktop virtual	Penyedia desktop virtual yang digunakan lingkungan ini.
Nama layanan desktop virtual	Pengidentifikasi unik yang diberikan penyedia layanan desktop virtual ke lingkungan ini.

Elemen	Deskripsi
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

WorkSpaces Lingkungan Thin Client dijalankan pada antarmuka desktop virtual. Setiap antarmuka memiliki serangkaian parameter berbeda yang mengontrol lingkungan khusus.

Detail WorkSpaces direktori Amazon

WorkSpaces Lingkungan Thin Client berjalan di Amazon WorkSpaces menggunakan direktori untuk membuat dan menjalankan desktop virtual mereka. Tabel berikut mencantumkan setiap elemen dalam rincian dan bagaimana fungsinya.

WorkSpaces directory details		
Directory ID abc	Organization name Name	Registered ✔ True
Directory name xyz	Directory type Simple AD	Status ✔ Active

Elemen	Deskripsi
ID Direktori	WorkSpaces Direktori Amazon yang terkait dengan lingkungan ini.
Nama Directory	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

WorkSpaces Lingkungan Thin Client berjalan di Amazon WorkSpaces Secure Browser menggunakan portal web untuk membuat dan menjalankan desktop virtual mereka. Tabel berikut mencantumkan setiap elemen dalam rincian dan bagaimana fungsinya.

WorkSpaces Web portal details		
Name Custom Web Portal - Mon, Mar 06, 2023, 12:00:51 🔗	Time created March 06, 2023, 13:50 (UTC-05:00)	Web portal endpoint

Elemen	Deskripsi
Nama	Pengenal unik yang terkait dengan portal Browser WorkSpaces Aman ini.
Waktu dibuat	Tanggal dan waktu ketika portal Browser WorkSpaces Aman ini dibuat.

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

WorkSpaces Rincian aplikasi

WorkSpaces Lingkungan Thin Client berjalan pada tumpukan informasi WorkSpaces Aplikasi untuk membuat dan menjalankan desktop virtual mereka. Tabel berikut mencantumkan setiap elemen dalam rincian dan bagaimana fungsinya.

AppStream 2.0 details		
Stack name xyz	IdP login url https://abc.com	Time created Thu Jun 08 2023 10:26:29 GMT-0700 (Pacific Daylight Time)

Elemen	Deskripsi
Nama tumpukan	Pengenal unik yang terkait dengan tumpukan WorkSpaces Aplikasi ini.
URL login iDP	Url penyedia identitas yang digunakan untuk masuk dan keluar dari tumpukan WorkSpaces Aplikasi Anda.
Waktu dibuat	Tanggal dan waktu ketika tumpukan WorkSpaces Aplikasi 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
- WorkSpaces Aplikasi melalui tumpukan yang ditetapkan
- 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](#)
- [Langkah 2: Pilih penyedia desktop virtual Anda](#)
- [Langkah 3: Kirim kode aktivasi ke pengguna perangkat Anda](#)

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](#)
- [WorkSpaces Aplikasi](#)

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 bahwa sistem Anda memenuhi persyaratan ini sebelum Anda mengatur konsol Anda.

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.
 - 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 WorkSpaces Aplikasi

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

⚠ Important

Untuk membuat lingkungan WorkSpaces Aplikasi, Anda harus `cli_follow_urlparam` menyetel 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 WorkSpaces Aplikasi, 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.
 - Buat tumpukan dengan memilih tombol **Create Stack**. Untuk informasi selengkapnya tentang membuat tumpukan WorkSpaces Aplikasi, 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.
 - 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

Ada sejumlah parameter untuk perangkat apa pun di jaringan Anda untuk Anda tinjau serta beberapa tindakan yang dapat Anda lakukan.

Devices
[Info](#)

Order devices

This is a list of all end user devices that you manage, including information about the user logins for each device.

Devices (1)

< 1 >

☐	Device ID	Device name	Activity status
☐	G0723H08	-	Active

Detail daftar perangkat

Parameter untuk perangkat Anda tercantum untuk ditinjau. Tabel berikut mencantumkan setiap elemen dalam ringkasan dan bagaimana fungsinya.

Elemen	Deskripsi
Nomor seri perangkat	Nomor identifikasi yang ditetapkan untuk perangkat individual.
Nama perangkat	(opsional) Nama unik yang Anda berikan ke perangkat.
Terakhir digunakan oleh	Nomor identifikasi pengguna yang mengakses perangkat. Hanya tersedia saat menggunakan WorkSpaces Personal.
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 akun AWS ini, dan

Elemen	Deskripsi
	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. • Deregistered — 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: • Sesuai • Tidak patuh

Tindakan daftar perangkat

Ada sejumlah tindakan yang dapat Anda lakukan dari sini. Pilih salah satu dari ini untuk melakukan tindakan yang sesuai.

Elemen	Deskripsi
Pencarian	Mencari 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](#)
- [Mengeksport detail perangkat](#)

Detail perangkat

Saat Anda memilih perangkat, konsol WorkSpaces Thin Client menampilkan detail untuk perangkat tersebut untuk Anda tinjau. Konsol juga menampilkan detail tentang jenis jaringan perangkat dan periferal yang terhubung.

Topik

- [Ringkasan](#)

- [Pengaturan perangkat](#)
- [Aktivitas Pengguna](#)

Ringkasan

Bagian Ringkasan memberikan ikhtisar tingkat tinggi tentang fitur-fitur utama perangkat Klien WorkSpaces Tipis. Tabel berikut mencantumkan setiap elemen dalam ringkasan dan bagaimana fungsinya.

Summary

Device serial number

ARN

Device name

Device type

Activity status

Environment ID

Enrollment status

Enrolled since

Last logged in

Last posture checked at

Current software version

Scheduled for software update

Software compliance

Elemen	Deskripsi
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

Elemen	Deskripsi
	• Nonaktif
ID Lingkungan	Nomor identifikasi lingkungan yang digunakan perangkat.
Status pendaftaran	Konfirmasi bahwa perangkat telah disiapkan , dikaitkan dengan akun AWS 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 saat ini tidak 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 .

Elemen	Deskripsi
Kepatuhan perangkat lunak	Konfirmasi bahwa set perangkat lunak valid. Ada dua status status: • Patuh • Tidak Patuh
Terakhir digunakan oleh	Nomor identifikasi pengguna yang mengakses perangkat. Hanya tersedia saat menggunakan WorkSpaces Personal.

Log pengguna

User activity details (5)
[Info](#)

[Export details](#)


< 1 >


Device accessed on ▼

August 28, 2023, 21:46 (UTC-04:00)

August 28, 2023, 18:18 (UTC-04:00)

August 24, 2023, 10:56 (UTC-04:00)

August 24, 2023, 10:56 (UTC-04:00)

August 24, 2023, 09:33 (UTC-04:00)

Elemen	Deskripsi
Akses perangkat terakhir	Tanggal dan waktu kapan perangkat ini terakhir digunakan.

Pengaturan perangkat

Parameter untuk perangkat Anda tercantum untuk ditinjau. Tabel berikut mencantumkan setiap elemen dan bagaimana fungsinya.

 **Note**

Informasi pengaturan perangkat diperbarui hanya ketika perangkat sedang online. Jika perangkat offline, beberapa informasi mungkin kedaluwarsa.

Judul dan Jaringan

WorkSpaces Detail perangkat Thin Client memberikan gambaran umum tentang koneksi jaringan perangkat. Tabel berikut mencantumkan setiap elemen dan bagaimana fungsinya.

Device settings [Info](#)

Last synced on: October 21, 2024, 14:28 (UTC-07:00)

▼ Network

Connection type

ETHERNET

Status

 Connected

Local IP address

Gateway address

Elemen	Deskripsi
Terakhir disinkronkan pada	Tanggal dan waktu pengaturan perangkat terbaru disinkronkan dengan konsol.
Tipe koneksi	Jenis koneksi jaringan yang digunakan oleh perangkat. Jenis koneksi dapat berupa Ethernet atau Wifi.
Status	Status jaringan. Jika perangkat saat ini terhubung, atau terhubung dalam 20 menit terakhir, status akan muncul sebagai 'terhubung'. Jika jaringan telah terputus selama lebih dari 20 menit, status akan berubah untuk menunjukkan waktu yang berlalu sejak perangkat terakhir terhubung ke internet,

Elemen	Deskripsi
	misalnya “terakhir terhubung 20 menit yang lalu”.
Alamat IP lokal	Alamat IP lokal dari jaringan yang terhubung.
Alamat gateway	Alamat gateway dari jaringan yang terhubung.

Bluetooth dan perangkat periferal

WorkSpaces Detail perangkat Thin Client memberikan daftar periferal yang terhubung ke perangkat. Tabel berikut mencantumkan setiap elemen dan bagaimana fungsinya.

▼ Bluetooth and peripheral devices	
Bluetooth ✔ Enabled	
Connected peripheral devices (5)	
Name	Type
Logitech USB Receiver Mouse	Mouse (USB)
Logitech USB Receiver	Keyboard (USB)
Plantronics Blackwire 5220 Series	Speaker (USB)
Plantronics Blackwire 5220 Series	Microphone (USB)
UVC Camera (046d:0825)	Webcam (USB)

Elemen	Deskripsi
Bluetooth	Status Bluetooth perangkat. Dua status status tersebut adalah: • Diaktifkan • Dinonaktifkan
Perangkat periferal yang terhubung	Daftar nama periferal yang terhubung, seperti mouse Logitech, dan jenis periferal yang terhubung, seperti Mouse (USB).

Kekuatan dan tidur

Setiap perangkat WorkSpaces Thin Client memiliki mode hemat daya. Tabel berikut mencantumkan status mode ini.

▼ Power and sleep

Turn off display after
Never

Elemen	Deskripsi
Matikan tampilan setelahnya	Periode waktu tidak aktif setelah perangkat mematikan tampilannya.

Aktivitas Pengguna

Tab ini menampilkan log informasi penyiapan dan penggunaan perangkat tertentu. Tabel berikut mencantumkan setiap elemen log ini.

User activity details (1) Info					
Filter by device accessed date and time		Find by attribute or keyword			
Device accessed on	User ID	Virtual desktop service	Virtual desktop service ID	IP address	Session ID
March 06, 2025, 16:43 (UTC+01:00)	sld-demo	WorkSpaces	d-123456abcde	2a02:a46a:9b7c:...	gw2-8a88e81

Elemen	Deskripsi
Perangkat diakses di	Tanggal dan waktu perangkat diaktifkan.
ID Pengguna	Nomor identifikasi pengguna yang mengakses perangkat.
Layanan desktop virtual	Layanan desktop virtual yang digunakan perangkat.
ID layanan desktop virtual	Nomor ID layanan desktop virtual yang terkait dengan pengguna.

Elemen	Deskripsi
Alamat IP	Nomor identifikasi IP yang mengakses perangkat.
Tipe peristiwa	Detail tentang bagaimana perangkat digunakan .

Note

Dengan pengecualian WorkSpaces Personal, VDIs hanya tampilkan peristiwa yang dimulai Login.

Anda dapat menggunakan bilah pencarian di atas tabel untuk menemukan informasi spesifik dalam tabel. Anda juga dapat memfilter hasil tabel berdasarkan tanggal dan waktu.

Anda dapat mengeksport tabel ke file csv dengan memilih tombol Ekspor detail.

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.

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.

Klien Amazon WorkSpaces Thin Anda - Data yang dihasilkan oleh penggunaan perangkat

Amazon WorkSpaces Thin Client Anda menghasilkan dan mengumpulkan data tentang interaksi Anda dengannya.

Jenis Data: Amazon WorkSpaces Thin Client Anda menghasilkan data tentang kinerja perangkat, pola penggunaan, dan interaksi dengan AWS layanan lain. Ini termasuk data teknis (seperti status dan pengaturan), data penggunaan (seperti stempel waktu masuk), dan data diagnostik (seperti log sistem jika relevan).

Volume & Pengumpulan Data: Jumlah data yang dihasilkan bervariasi berdasarkan cara Anda menggunakan perangkat dan layanan Anda. Data dikumpulkan terus menerus selama pengoperasian perangkat.

Penyimpanan Data: Data dari perangkat Anda disimpan dengan aman di perangkat itu sendiri atau di AWS server. Itu disimpan dalam format terstruktur dan dapat dibaca mesin.

Akses Data: Anda dapat mengakses data perangkat Anda melalui AWS akun Anda mengikuti petunjuk yang tercantum [di sini](#). Informasi lebih lanjut, termasuk instruksi tentang unduhan data dan informasi tentang kualitas layanan, tersedia di [halaman](#) ini.

Manajemen Data: Anda dapat meninjau data perangkat Anda melalui AWS akun Anda. Untuk mempelajari lebih lanjut tentang praktik data perangkat Anda, silakan tinjau [Ketentuan Layanan](#) dan [Pemberitahuan Privasi](#) kami.

Penghapusan Data: Anda dapat menghapus data perangkat Anda melalui akun Anda AWS . Untuk informasi tentang opsi penyimpanan dan penghapusan data, kunjungi [Menghapus perangkat](#).

Berbagi data dengan orang lain: AWS tidak membagikan data perangkat Anda dengan pihak ketiga. Hanya pihak ketiga yang berwenang yang dapat mengakses data Anda setelah persetujuan Anda

melalui proses [Identifikasi dan Manajemen Akses](#) kami. AWS membagikan data pribadi dengan pihak ketiga dalam kasus terbatas yang termasuk dalam [Pemberitahuan AWS Privasi](#).

Butuh Bantuan? Kunjungi [Customer Support](#) untuk menghubungi tim dukungan kami. Ini tanpa mengurangi hak Anda untuk mengajukan keluhan berdasarkan hukum yang berlaku.

Pemegang data: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luksemburg

Pembaruan perangkat lunak

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

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

Ada dua jenis perangkat lunak:

- Perangkat lunak yang memperkenalkan fungsionalitas baru, memperbaiki cacat, dan melakukan perbaikan umum. Ini dirilis setiap bulan.
- Perangkat lunak yang berisi tambalan keamanan dan perbaikan untuk masalah kritis. Ini dirilis sesuai kebutuhan.

Sebagai administrator, jika Anda belum mengaktifkan pembaruan perangkat lunak otomatis di lingkungan Anda, perangkat yang terdaftar di lingkungan tersebut tidak akan menerima pembaruan perangkat lunak hingga Anda mendorong pembaruan secara manual.

Saat perangkat lunak baru dirilis, perangkat lunak yang lebih lama kedaluwarsa. Mulai dari tanggal rilis perangkat lunak yang ditetapkan dengan fungsionalitas baru, Anda memiliki 40 hari sebelum perangkat lunak sebelumnya kedaluwarsa.

Untuk memastikan postur keamanan perangkat tetap utuh, layanan secara otomatis memperbarui perangkat jika mendeteksi perangkat lunak yang kedaluwarsa. Jenis pembaruan ini dapat mengganggu sesi aktif karena tidak akan menghormati jendela pemeliharaan atau memungkinkan

pengguna akhir untuk menunda pembaruan. Untuk menghindari hal ini, kami sarankan memperbarui perangkat lunak setidaknya sekali setiap 30 hari.

Note

Jika Perangkat Lunak yang disetel dengan tambalan keamanan atau pembaruan penting dirilis, semua set Perangkat Lunak sebelumnya akan ditetapkan untuk kedaluwarsa dalam 3 hari. Untuk memastikan perangkat Anda tetap aman dan meminimalkan gangguan pada operasi harian, kami sarankan untuk segera memperbarui set Perangkat Lunak ini.

Lihat [set perangkat lunak lingkungan Klien WorkSpaces Tipis](#) untuk daftar Set Perangkat Lunak yang dirilis.

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
2.20.1	11-18-2025	Perbaiki untuk masalah keamanan kritis CVE-2025-13223 dan CVE-2025-13224 Chromium.
2.20.0	11-5-2025	Meningkatkan otentikasi perangkat.
2.19.0	9-30-2025	- Tindakan toolbar seperti Restart, Shut down, dan Sleep sekarang mengharuskan pengguna akhir untuk mengautentikasi ulang. WorkSpaces - Memperbaiki masalah saat pengguna akhir tidak dapat menggunakan tombol Ctrl +Spasi untuk memilih kolom di Excel. - Mengubah internal URLs untuk halaman Kunci dan Lisensi.
2.18.0	8-28-2025	- Menambahkan tombol Exit Session ke toolbar perangkat. - Memperbaiki masalah saat pemberitahuan status aktivitas salah ditampilkan di perangkat.

Set perangkat lunak	Tanggal rilis	Perubahan
		• Ditambahkan dukungan untuk otentikasi FIDO2 dalam sesi. • Perbaikan dan perbaikan umum.
2.17.0	7-30-2025	• Hub USB plugable UD-3900Z sekarang didukung untuk digunakan dengan Thin Client WorkSpaces • Menambahkan dukungan untuk AltGr tombol dengan keyboard Spanyol. • Memperbaiki masalah yang mengakibatkan entri duplikat untuk aktivitas sesi pengguna untuk perangkat. • Ditambahkan dukungan untuk tombol Enter pada keypad numerik. • Perbaikan dan perbaikan umum.
2.16.2	7-22-2025	• Perbaiki untuk masalah keamanan kritis CVE-2025-6558 Chromium.
2.16.1	7-3-2025	• Perbaiki untuk masalah keamanan kritis CVE-2025-6554 Chromium.

Set perangkat lunak	Tanggal rilis	Perubahan
2.16.0	6-27-2025	• Menambahkan pemberitahuan untuk Latensi Jaringan. • Ditambahkan kemampuan untuk pulih dari monitor kedua menjadi gelap selama sesi. • Memperbaiki masalah dengan monitor yang menampilkan layar putih atau tidak diperpanjang secara otomatis setelah perangkat kembali dari mode tidur.
2.15.0	6-19-2025	• Ditambahkan dukungan untuk keyboard Amerika Latin Spanyol dan Inggris Internasional. • Pengguna akhir melihat notifikasi saat perangkat tidak mendeteksi aktivitas keyboard atau mouse untuk waktu yang lama.
2.14.1	6-09-2025	• Perbaiki untuk masalah keamanan kritis CVE-2025-5419 Chromium.

Set perangkat lunak	Tanggal rilis	Perubahan
2.13.0	3-31-2025	• Pengguna akhir akan melihat survei umpan balik kepuasan produk sebagai pemberitahuan. • Menambahkan dukungan fitur prarilis untuk FIDO2 aliran otentikasi. Lihat detail FIDO2 pra-sesi. • Perangkat tidak akan tidur jika audio/video diputar di sesi. • Pengguna akhir melihat notifikasi saat monitor terhubung dan terputus. • Perangkat mengumpulkan informasi diagnostik dari sistem operasi untuk peningkatan layanan. • Memperbaiki masalah saat tanggal yang salah ditampilkan di Pengaturan untuk tanggal penginstalan perangkat lunak.
2.14.0	4-29-2025	• Peningkatan kegunaan dan perbaikan bug.

Set perangkat lunak	Tanggal rilis	Perubahan
2.13.0	3-31-2025	- Pengguna akhir akan melihat survei umpan balik kepuasan produk sebagai pemberitahuan. - Menambahkan dukungan fitur prarilis untuk FIDO2 aliran otentikasi. Lihat detail FIDO2 pra-sesi. - Perangkat tidak akan tidur jika audio/video diputar di sesi. - Pengguna akhir melihat notifikasi saat monitor terhubung dan terputus. - Perangkat mengumpulkan informasi diagnostik dari sistem operasi untuk peningkatan layanan. - Memperbaiki masalah saat tanggal yang salah ditampilkan di Pengaturan untuk tanggal penginstalan perangkat lunak.
2.12.0	1-30-2025	Memperbaiki masalah saat pengguna akhir keluar dari sesi saat menekan tombol kembali pada mouse.
2.11.2	1-24-2025	Memperbaiki masalah saat audio berderak selama panggilan dengan gerakan mouse di seluruh monitor.

Set perangkat lunak	Tanggal rilis	Perubahan
2.11.1	12-27-2024	• Memperbaiki masalah perpanjangan otomatis monitor ganda. • Perbaikan kecil pada VoiceView label.
2.11.0	12-19-2024	• WorkSpaces Thin Client sekarang mendukung VoiceView dan Magnifier.
2.10.0	11-22-2024	• Pengguna akhir dapat menggunakan pintasan keyboard untuk menutup bilah alat perangkat.

Set perangkat lunak	Tanggal rilis	Perubahan
2.9.0	10-28-2024	• Administrator sekarang dapat melihat setelan perangkat pengguna akhir mereka dalam AWS konsol di bawah halaman Detail perangkat perangkat tertentu. • WorkSpaces Thin Client sekarang mendukung monitor resolusi 2K untuk satu layar. • Pengguna akhir dapat melihat notifikasi yang terkait dengan diagnostik jaringan pada perangkat WorkSpaces Thin Client mereka. • Pengguna akhir sekarang dapat memilih untuk menempatkan toolbar perangkat di kiri atau kanan sesuai preferensi mereka. • Memperbaiki masalah saat perangkat tidak menginstal pembaruan perangkat lunak selama waktu tidur atau idle.
2.8.1	09-26-2024	• Memperbaiki masalah kritis di mana monitor kedua tidak dapat diaktifkan setelah perangkat bangun dari tidur.

Set perangkat lunak	Tanggal rilis	Perubahan
2.8.0	09-06-2024	• Thin Client mendukung monitor dengan resolusi 4K. • Pengguna dapat terhubung ke sesi VDI meskipun layanan manajemen perangkat WorkSpaces Thin Client sementara tidak tersedia. • Memperbaiki masalah saat bagian detail aktivitas Pengguna di AWS konsol menunjukkan entri duplikat. • Pengguna akhir dapat menggunakan PrintScreen opsi saat streaming WorkSpaces di WorkSpaces Thin Client.
2.7.1	08-27-2024	• Perbaikan zero-day untuk masalah keamanan kritis CVE-2024-7971 dan CVE-2024-7965 Chromium.
2.7.0	07-29-2024	• Perbaikan kinerja monitor kedua. • Memperbaiki masalah saat bahasa bilah alat tidak terpengaruh saat mengubah bahasa perangkat. • Perangkat sekarang mengumpulkan informasi diagnostik untuk peningkatan layanan.

Set perangkat lunak	Tanggal rilis	Perubahan
2.6.0	07-09-2024	• Pengguna dapat menunda pembaruan perangkat lunak yang masuk sehingga mereka dapat menyelesaikan pekerjaan mereka tanpa gangguan. • Pengaturan perangkat memungkinkan pengguna untuk melupakan WiFi jaringan yang disimpan. • Perbaiki kinerja audio/video panggilan dalam sesi. • Beberapa pengaturan pengguna untuk sesi VDI tetap ada di seluruh perangkat reboot.
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. • Perbaiki kinerja audio/video panggilan dalam sesi.
2.4.3	05-29-2024	• Perbaiki 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 sesi IDP untuk Aplikasi. WorkSpaces • 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 SAMP 2.0.

Set perangkat lunak	Tanggal rilis	Perubahan
2.2.0	02-08-2024	Menambahkan dukungan untuk keyboard ISO dengan bahasa Inggris (Britania Raya), Prancis, Jerman, Italia, Spanyol.
2.1.2	01-26-2024	- Perbaikan nol hari 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 memungkinkan dukungan untuk tombol Meta. Hal ini memungkinkan 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.
- Anda dapat mengonfigurasi tag untuk perangkat di lingkungan agar diterapkan secara otomatis saat Anda mendaftarkan perangkat.

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 mengelola 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 mengelola 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 mengelola tag untuk perangkat baru dengan menggunakan konsol

1. Buka [konsol WorkSpaces Thin Client](#).
2. Pilih Lingkungan untuk membuka halaman detailnya.
3. Pilih Edit.
4. Di bagian Tag pembuatan perangkat, 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.

Ketika perangkat dibuat, itu terdaftar dengan lingkungan dan tag pembuatan perangkat diterapkan. Ini hanya terjadi selama pendaftaran perangkat baru. Selain itu, tag `aws:thinclient:environment-id` sistem diterapkan dengan Id lingkungan yang digunakan sebagai nilai.

Untuk mengelola 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](#)
- [Manajemen identitas dan akses untuk Amazon WorkSpaces Thin Client](#)
- [Ketahanan di Amazon WorkSpaces Thin Client](#)
- [Analisis dan manajemen kerentanan di Amazon WorkSpaces Thin Client](#)

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 kredensial 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 AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan WorkSpaces Thin Client atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. 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, kredensial 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](#)
- [Enkripsi data saat istirahat untuk Amazon WorkSpaces Thin Client](#)
- [Enkripsi saat bergerak](#)
- [Manajemen kunci](#)
- [Privasi lalu lintas kerja internet](#)

Enkripsi data

WorkSpaces Thin Client mengumpulkan data kustomisasi lingkungan dan perangkat, seperti pengaturan pengguna, pengidentifikasi perangkat, informasi penyedia identitas, dan pengenalan 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 kredensial pengguna:
 - Admin diminta untuk masuk ke konsol WorkSpaces Thin Client, dan pengguna diharuskan untuk memberikan kode aktivasi untuk penyiapan WorkSpaces Thin Client menggunakan kredensial 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 kredensial 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 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
Aktivitas pengguna WorkSpaces Aktivitas Pengguna Klien Tipis	Diaktifkan	Diaktifkan
Pengaturan perangkat WorkSpaces Pengaturan Perangkat Klien Tipis	Diaktifkan	Diaktifkan
Tag pembuatan perangkat	Diaktifkan	Diaktifkan

Jenis data	Enkripsi kunci yang dimiliki AWS	Enkripsi kunci yang dikelola pelanggan (Opsional)
WorkSpaces Tag pembuatan perangkat Thin Client Environment		

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 AWS KMS

Amazon WorkSpaces Thin Client memerlukan kebijakan utama agar Anda dapat menggunakan kunci yang dikelola pelanggan.

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

- Kirim [GenerateDataKey](#) permintaan ke AWS KMS untuk mengenkripsi data.
- Kirim [Decrypt](#) permintaan ke AWS KMS untuk mendekripsi data terenkripsi.

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 WorkSpaces Thin Client, maka operasi akan mengembalikan `AccessDeniedException` kesalahan. Selain itu, perangkat WorkSpaces Thin Client tidak akan dapat menggunakan WorkSpaces Thin Client Environment.

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.

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"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "kms:ViaService": "thinclient.region.amazonaws.com",
                "kms:CallerAccount": "111122223333"
            }
        }
    },
    {
        "Sid": "Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt
data",
        "Effect": "Allow",
        "Principal": {"Service": "thinclient.amazonaws.com"},
        "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "aws:SourceArn":
                    "arn:aws:thinclient:region:111122223333:*",
                "kms:EncryptionContext:aws:thinclient:arn":
                    "arn:aws:thinclient:region: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*"
    ],
    "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 menyediakankmsKeyArn, 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.

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`, `GenerateDataKeyDecrypt`, 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": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "attributes": {

```

```

        "creationDate": "2024-04-08T13:43:33Z",
        "mfaAuthenticated": "false"
    },
    "invokedBy": "thinclient.amazonaws.com"
},
"eventTime": "2024-04-08T13:44:22Z",
"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"
}

```

GenerateDataKey

Amazon WorkSpaces Thin Client menggunakan GenerateDataKey operasi untuk mengenkripsi data.

Contoh peristiwa berikut mencatat GenerateDataKey operasi:

```

{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",

```

```

    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-04-08T12:21:03Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2024-04-08T13:03:56Z",
  "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",
  "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
  "vpceEndpointId": "vpce-1234abcd567SAMPLE",
  "vpceEndpointAccountId": "thinclient.amazonaws.com",
  "eventCategory": "Management"
}

```

GenerateDataKey (by service)

Saat Amazon WorkSpaces Thin Client menggunakan informasi Perangkat GenerateDataKey penyimpanan, GenerateDataKey operasi digunakan untuk mengenkripsi data.

GenerateDataKeyOperasi diizinkan dalam pernyataan kebijakan kunci KMS dengan Sid “Izinkan layanan Amazon WorkSpaces Thin Client untuk mengenkripsi dan mendekripsi data”.

Contoh peristiwa berikut mencatat GenerateDataKey operasi:

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2024-04-08T13:03:56Z",
  "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",
  "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
  "vpcEndpointId": "vpce-1234abcd567SAMPLE",
  "vpcEndpointAccountId": "thinclient.amazonaws.com",
  "eventCategory": "Management"
}

```

Decrypt

Amazon WorkSpaces Thin Client menggunakan Decrypt operasi untuk mendekripsi data.

Contoh peristiwa berikut mencatat Decrypt operasi:

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      }
    }
  }
}

```

```

    },
    "attributes": {
      "creationDate": "2024-04-08T13:43:33Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "thinclient.amazonaws.com"
},
"eventTime": "2024-04-08T13:44:25Z",
"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",
"sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
"vpceEndpointId": "vpce-1234abcd567SAMPLE",
"vpceEndpointAccountId": "thinclient.amazonaws.com",
"eventCategory": "Management"

```

}

Decrypt (by service)

Ketika Perangkat Klien WorkSpaces Tipis mengakses informasi Lingkungan atau Perangkat, Decrypt operasi digunakan untuk mendekripsi data. DecryptOperasi diizinkan dalam pernyataan kebijakan kunci KMS dengan Sid “Izinkan layanan Amazon WorkSpaces Thin Client untuk mengenkripsi dan mendekripsi data”.

Contoh peristiwa berikut mencatat Decrypt operasi, yang diotorisasi melaluiGrant:

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2024-04-08T13:44:25Z",
  "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",
"sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
"vpceEndpointId": "vpce-1234abcd567SAMPLE",
"vpceEndpointAccountId": "thinclient.amazonaws.com",
"eventCategory": "Management"
}
```

Pelajari Lebih Lanjut

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 saat 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 WorkSpaces Aplikasi](#), 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](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Amazon WorkSpaces Thin Client bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Amazon Thin Client WorkSpaces](#)
- [AWS kebijakan terkelola untuk Amazon WorkSpaces Thin Client](#)
- [Memecahkan masalah identitas dan akses Amazon WorkSpaces Thin Client](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Memecahkan masalah identitas dan akses Amazon WorkSpaces Thin Client](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana Amazon WorkSpaces Thin Client bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Contoh kebijakan berbasis identitas untuk Amazon Thin Client WorkSpaces](#))

Mengautentikasi dengan identitas

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

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensial Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensi dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center.

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna gabungan, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon. EC2 Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukannya.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih 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. Contohnya termasuk 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. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

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.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — Tentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .

- Kebijakan kontrol sumber daya (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan 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 kondisi kebijakan	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya

Fitur IAM	WorkSpaces Dukungan Klien Tipis
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 oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan 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 tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam 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, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk 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:

```
thinclient
```

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

```
"Action": [  
    "thinclient:action1",  
    "thinclient: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, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"

```

Untuk melihat daftar jenis sumber daya Klien WorkSpaces Tipis dan jenisnya ARNs, lihat Sumber Daya yang [Ditetapkan 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 khusus layanan: Yes

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

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. 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](#)

ACLs di WorkSpaces Thin Client

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka 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 tanda. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

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

Untuk informasi selengkapnya tentang ABAC, lihat [Tentukan izin dengan otorisasi ABAC](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) dalam Panduan Pengguna IAM.

Menggunakan kredensi sementara dengan WorkSpaces Thin Client

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. 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](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

Izin utama lintas layanan untuk WorkSpaces Klien Tipis

Mendukung sesi akses terusan (FAS): Ya

Sesi akses terusan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

Peran layanan untuk Klien WorkSpaces Tipis

Mendukung peran layanan: Tidak

Peran layanan adalah [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 [Buat sebuah 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 tersebut dapat menjalankan 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 manajemen peran terkait layanan, lihat [Layanan AWS yang berfungsi dengan IAM](#). Cari layanan dalam tabel yang memiliki Yes di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Amazon Thin Client WorkSpaces

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Klien WorkSpaces Tipis. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM \(konsol\) di Panduan Pengguna IAM](#).

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Klien WorkSpaces Tipis, termasuk format ARNs 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](#)
- [Mengizinkan 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 membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam 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 melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi

tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu 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 CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – 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 dengan IAM Access Analyzer](#) dalam 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 meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam 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. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

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.

JSON

```
{
  "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/*"]
    }
}

```

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan 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.

JSON

```

{
  "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/*"]
    }
  ]
}

```

```
}  
]
```

AWS kebijakan terkelola untuk Amazon WorkSpaces Thin Client

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AmazonWorkSpacesThinClientReadOnlyAccess

Anda dapat melampirkan kebijakan AmazonWorkSpacesThinClientReadOnlyAccess ke identitas IAM Anda. Kebijakan ini memberikan izin akses penuh ke layanan Klien WorkSpaces Tipis dan dependensinya. Untuk informasi selengkapnya tentang kebijakan terkelola ini, lihat [AmazonWorkSpacesThinClientReadOnlyAccess](#) di panduan Referensi Kebijakan AWS Terkelola.

Detail izin

Kebijakan ini mencakup izin berikut.

- `thinclient(WorkSpaces Thin Client)` - Memungkinkan akses read-only ke semua tindakan WorkSpaces Thin Client.
- `workspaces(WorkSpaces)` — Memungkinkan izin untuk menggambarkan WorkSpaces direktori dan alias koneksi. Ini digunakan untuk memeriksa apakah WorkSpaces sumber daya Anda

kompatibel dengan WorkSpaces Thin Client. Ini juga digunakan untuk menunjukkan sumber daya ini di AWS konsol WorkSpaces Thin Client.

- **workspaces-web**(WorkSpaces Secure Browser) — Memungkinkan izin untuk menggambarkan WorkSpaces Secure Browser portal dan pengaturan pengguna. Ini digunakan untuk memeriksa apakah WorkSpaces Secure Browser sumber daya Anda kompatibel dengan WorkSpaces Thin Client. Ini juga digunakan untuk menunjukkan sumber daya ini di AWS konsol WorkSpaces Thin Client.
- **appstream**(WorkSpaces Aplikasi) - Memungkinkan izin untuk menggambarkan tumpukan WorkSpaces Aplikasi. Ini digunakan untuk memeriksa apakah sumber daya WorkSpaces Aplikasi Anda kompatibel dengan WorkSpaces Thin Client. Ini juga digunakan untuk menunjukkan sumber daya ini di AWS konsol WorkSpaces Thin Client.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowWorkSpacesSecureBrowserAccess",
    "Effect": "Allow",
    "Action": [
      "workspaces-web:GetPortal",
      "workspaces-web:GetUserSettings",
      "workspaces-web:ListPortals"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowAppStreamAccess",
    "Effect": "Allow",
    "Action": [
      "appstream:DescribeStacks"
    ],
    "Resource": "*"
  }
]
}

```

AWS kebijakan terkelola: AmazonWorkSpacesThinClientFullAccess

Anda dapat melampirkan kebijakan AmazonWorkSpacesThinClientFullAccess ke identitas IAM Anda. Kebijakan ini memberikan izin akses penuh ke layanan Klien WorkSpaces Tipis dan dependensinya. Untuk informasi selengkapnya tentang kebijakan terkelola ini, lihat [AmazonWorkSpacesThinClientFullAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

Detail izin

Kebijakan ini mencakup izin berikut:

- `thinclient`(WorkSpaces Thin Client) - Memungkinkan akses penuh ke semua tindakan WorkSpaces Thin Client.
- `workspaces`(WorkSpaces) — Memungkinkan izin untuk menggambarkan WorkSpaces direktori dan alias koneksi. Ini digunakan untuk memeriksa apakah WorkSpaces sumber daya Anda kompatibel dengan WorkSpaces Thin Client. Ini juga digunakan untuk menunjukkan sumber daya ini di AWS konsol WorkSpaces Thin Client.

- **workspaces-web**(WorkSpaces Secure Browser) — Memungkinkan izin untuk menggambarkan WorkSpaces Secure Browser portal dan pengaturan pengguna. Ini digunakan untuk memeriksa apakah WorkSpaces Secure Browser sumber daya Anda kompatibel dengan WorkSpaces Thin Client. Ini juga digunakan untuk menunjukkan sumber daya ini di AWS konsol WorkSpaces Thin Client.
- **appstream**(WorkSpaces Aplikasi) - Memungkinkan izin untuk menggambarkan tumpukan WorkSpaces Aplikasi. Ini digunakan untuk memeriksa apakah sumber daya WorkSpaces Aplikasi Anda kompatibel dengan WorkSpaces Thin Client. Ini juga digunakan untuk menunjukkan sumber daya ini di AWS konsol WorkSpaces Thin Client.
- **iam**— Memungkinkan Klien WorkSpaces Tipis untuk membuat peran terkait layanan di akun Anda. Peran ini memungkinkan Klien WorkSpaces Tipis untuk mempublikasikan metrik atas nama Anda. CloudWatch

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientFullAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
```

```

        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowAppStreamAccess",
    "Effect": "Allow",
    "Action": [
        "appstream:DescribeStacks"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowCreateServiceLinkedRole",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "monitoring.thinclient.amazonaws.com"
        }
    }
}
]
}

```

WorkSpaces Pembaruan Klien Tipis ke kebijakan AWS terkelola

Ubah	Deskripsi	Date
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy— Kebijakan yang dihapus	WorkSpaces Thin Client menghapus AmazonWorkSpacesThinClientMonitoringServiceRolePolicy bagian tersebut.	November 12, 2025

Ubah	Deskripsi	Date
AmazonWorkSpacesThinClientFullAccess — Kebijakan yang diperbarui AmazonWorkSpacesThinClientMonitoringServiceRolePolicy – Kebijakan baru	WorkSpaces Thin Client memperbarui kebijakan untuk menyertakan peran terkait layanan.	26 Agustus 2025
AmazonWorkSpacesThinClientReadOnlyAccess — Kebijakan yang diperbarui	WorkSpaces Klien Tipis memperbarui kebijakan untuk menyertakan izin baca terbatas untuk detail perangkat dan alias WorkSpaces koneksi.	9 Januari 2025
AmazonWorkSpacesThinClientFullAccess — Kebijakan yang diperbarui	WorkSpaces Klien Tipis memperbarui kebijakan untuk menyertakan izin baca terbatas untuk alias WorkSpaces koneksi.	9 Januari 2025
AmazonWorkSpacesThinClientReadOnlyAccess — Kebijakan yang diperbarui	WorkSpaces Thin Client memperbarui kebijakan untuk menyertakan izin baca terbatas untuk WorkSpaces Aplikasi, WorkSpaces Web, dan WorkSpaces.	9 Agustus 2024
AmazonWorkSpacesThinClientFullAccess – Kebijakan baru	Menyediakan akses penuh ke Amazon WorkSpaces Thin Client serta akses terbatas ke layanan terkait yang diperlukan.	9 Agustus 2024

Ubah	Deskripsi	Date
AmazonWorkSpacesThinClientReadOnlyAccess – Kebijakan baru	Menyediakan akses hanya-baca ke Amazon WorkSpaces Thin Client dan dependensinya.	19 Juli 2024
WorkSpaces Thin Client mulai melacak perubahan	WorkSpaces Thin Client mulai melacak perubahan untuk kebijakan yang AWS dikelola.	19 Juli 2024

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 Konsol Manajemen AWS memberitahu Anda bahwa Anda tidak berwenang untuk melakukan suatu tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi 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 `thinclient:ListDevices`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
thinclient: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 `thinclient: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 memberikan izin kepada orang atau aplikasi yang membutuhkan akses. Jika Anda menggunakan AWS IAM Identity Center untuk mengelola orang dan aplikasi, Anda menetapkan set izin kepada pengguna atau grup untuk menentukan tingkat akses mereka. Set izin secara otomatis membuat dan menetapkan kebijakan IAM ke peran IAM yang terkait dengan orang atau aplikasi. Untuk informasi selengkapnya, lihat [Set izin](#) di Panduan AWS IAM Identity Center Pengguna.

Jika Anda tidak menggunakan IAM Identity Center, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Anda kemudian harus melampirkan kebijakan ke entitas yang memberi mereka izin yang benar di WorkSpaces Thin Client. Setelah izin diberikan, berikan kredensialnya kepada pengguna atau pengembang aplikasi. Mereka akan menggunakan kredensi tersebut untuk mengakses. AWS Untuk mempelajari selengkapnya tentang membuat pengguna, grup, kebijakan, dan izin IAM, lihat [Identitas dan Kebijakan IAM dan izin di IAM 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 orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah WorkSpaces Thin Client mendukung fitur-fitur ini, lihat [Bagaimana 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 [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM 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 secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

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 Aplikasi WorkSpaces Amazon, dan WorkSpaces Web. Lihat tautan berikut untuk informasi selengkapnya tentang manajemen pembaruan untuk masing-masing layanan ini:

- [Perbarui Manajemen di WorkSpaces Aplikasi Amazon](#)
- [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 CloudTrail menangkap 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, silakan lihat [Panduan Pengguna AWS CloudTrail](#).

Topik

- [Mencatat panggilan Amazon WorkSpaces Thin Client API menggunakan AWS CloudTrail](#)
- [Pantau WorkSpaces Thin Client Anda menggunakan CloudWatch metrik](#)

Mencatat panggilan Amazon WorkSpaces Thin Client API menggunakan AWS CloudTrail

Amazon WorkSpaces Thin Client terintegrasi dengan [AWS CloudTrail](#), layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. 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. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk WorkSpaces Thin Client, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

Semua tindakan Amazon WorkSpaces Thin Client dicatat oleh CloudTrail dan didokumentasikan dalam [Referensi API Amazon WorkSpaces Thin Client](#). Misalnya, panggilan ke `CreateEnvironment`, `DeleteDevice` dan `GetSoftwareSet` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat [Bekerja dengan riwayat CloudTrail Acara](#) di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara [CloudTrailDanau](#).

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan Konsol Manajemen AWS Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat [Membuat jejak untuk Anda Akun AWS](#) dan [Membuat jejak untuk organisasi](#) di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat [AWS CloudTrail Harga](#). Untuk informasi tentang harga Amazon S3, lihat [Harga Amazon S3](#).

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail [Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC](#). ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda

pilih dengan menerapkan pemilih acara [tingkat lanjut](#). Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Dana, lihat [Bekerja dengan AWS CloudTrail Dana](#) di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara dana dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih [opsi harga](#) yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat [AWS CloudTrail Harga](#).

WorkSpaces Peristiwa data Klien Tipis di CloudTrail

[Peristiwa data](#) memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya (misalnya, pendaftaran perangkat oleh pengguna akhir). Ini juga dikenal sebagai operasi bidang data. Peristiwa data seringkali merupakan aktivitas volume tinggi. Secara default, CloudTrail tidak mencatat peristiwa data. Riwayat CloudTrail peristiwa tidak merekam peristiwa data.

Biaya tambahan berlaku untuk peristiwa data. Untuk informasi selengkapnya tentang CloudTrail harga, lihat [AWS CloudTrail Harga](#).

Anda dapat mencatat peristiwa data untuk tipe resource WorkSpaces Thin Client menggunakan CloudTrail konsol AWS CLI, atau operasi CloudTrail API. Untuk informasi selengkapnya tentang cara mencatat peristiwa data, lihat [Mencatat peristiwa data dengan Konsol Manajemen AWS](#) dan Mencatat [peristiwa data dengan AWS Command Line Interface](#) di Panduan AWS CloudTrail Pengguna.

Tabel berikut mencantumkan tipe sumber daya WorkSpaces Thin Client yang dapat Anda log peristiwa data. Kolom tipe peristiwa data (konsol) menunjukkan nilai yang akan dipilih dari daftar tipe peristiwa Data di CloudTrail konsol. Kolom nilai resources.type menunjukkan **resources.type** nilai, yang akan Anda tentukan saat mengonfigurasi penyeleksi acara lanjutan menggunakan or. AWS CLI CloudTrail APIs CloudTrailKolom Data yang APIs dicatat ke menampilkan panggilan API yang dicatat CloudTrail untuk jenis sumber daya.

Jenis peristiwa data (konsol)	nilai resources.type	Data APIs masuk CloudTrail
ThinClientDevice	AWS::WorkSpacesThinClient::Device	- RegisterDevice - UpdateDeviceDetails

Anda dapat mengonfigurasi pemilih acara lanjutan untuk memfilter pada `eventNameReadOnly`, dan `resources`. ARN bidang untuk mencatat hanya peristiwa yang penting bagi Anda. Untuk informasi selengkapnya tentang bidang ini, lihat [AdvancedFieldSelector](#) di Referensi API AWS CloudTrail.

WorkSpaces Acara manajemen Klien Tipis di CloudTrail

[Acara manajemen](#) memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Akun AWS. Ini juga dikenal sebagai operasi pesawat kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

Amazon WorkSpaces Thin Client mencatat semua operasi bidang kontrol Klien WorkSpaces Tipis sebagai peristiwa manajemen. Untuk daftar operasi bidang kontrol Amazon WorkSpaces Thin Client yang dicatat oleh WorkSpaces Thin Client CloudTrail, lihat [Referensi API Amazon WorkSpaces Thin Client](#).

WorkSpaces Contoh acara Thin Client

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

Contoh berikut menunjukkan CloudTrail peristiwa yang menunjukkan RegisterDevice operasi.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "111111111111",
    "userName": "DSN: G1X11X11111111XX"
  },
  "eventTime": "2024-06-19T17:13:44Z",
  "eventSource": "thinclient.amazonaws.com",
  "eventName": "RegisterDevice",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "dsn": "G1X11X11111111XX",
    "activationCode": "xxx1xxx1",
    "model": "AFTGAZL"
  }
}
```

```

    },
    "responseElements": null,
    "requestID": "f626fb2b-a841-4b87-9a9b-685a62024058",
    "eventID": "214385d7-9249-4f60-af56-b4c951e0491d",
    "readOnly": false,
    "resources": [
      {
        "type": "AWS::ThinClient::Device",
        "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111111111111",
    "eventCategory": "Data"
  }
}

```

Contoh berikut menunjukkan CloudTrail peristiwa yang menunjukkan UpdateDeviceDetails operasi.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "111111111111",
    "userName": "DSN: G1X11X11111111XX"
  },
  "eventTime": "2024-10-21T17:46:27Z",
  "eventSource": "thinclient.amazonaws.com",
  "eventName": "UpdateDeviceDetails",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "7d562fcf-a9ce-40da-9e5c-9ef390b8b83c",
  "eventID": "f294b614-b00c-45ef-b293-cd389121033a",
  "readOnly": false,
  "resources": [
    {
      "type": "AWS::ThinClient::Device",
      "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
    }
  ]
}

```

```
],
"eventType": "AwsServiceEvent",
"managementEvent": false,
"recipientAccountId": "111111111111",
"serviceEventDetails": {
  "settings": {
    "network": {
      "ethernet": {
        "addresses": [
          {
            "gateway": "gateway",
            "localIp": "localIp",
            "type": "IPV4"
          }
        ],
        "connectionStatus": "NOT_CONNECTED"
      },
      "networkInterfaceInUse": "ETHERNET",
      "wifi": {
        "addresses": [
          {
            "gateway": "gateway",
            "localIp": "localIp",
            "type": "IPV4"
          }
        ],
        "connectionStatus": "NOT_CONNECTED"
      }
    },
    "peripherals": {
      "bluetooth": {
        "enabledStatus": "ENABLED"
      },
      "keyboards": [
        {
          "name": "name",
          "type": "USB"
        }
      ],
      "mice": [
        {
          "name": "name",
          "type": "BLUETOOTH"
        }
      ]
    }
  }
}
```

```
    ],
    "sound": {
      "microphones": [
        {
          "name": "name",
          "selectionStatus": "SELECTED",
          "type": "BUILT_IN"
        }
      ],
      "speakers": [
        {
          "name": "name",
          "selectionStatus": "SELECTED",
          "type": "BUILT_IN"
        }
      ]
    },
    "webcams": [
      {
        "name": "name",
        "selectionStatus": "SELECTED",
        "type": "USB"
      }
    ],
    "powerAndSleep": {
      "sleepAfter": "FIFTEEN_MINUTES"
    },
    "updatedAt": "2024-10-21T17:46:27.624Z"
  },
  "eventCategory": "Data"
}
```

Untuk informasi tentang konten CloudTrail rekaman, lihat [konten CloudTrail rekaman](#) di Panduan AWS CloudTrail Pengguna.

Pantau WorkSpaces Thin Client Anda menggunakan CloudWatch metrik

WorkSpaces Perangkat Thin Client dan Amazon CloudWatch terintegrasi, sehingga Anda dapat mengumpulkan dan menganalisis metrik kinerja yang dipancarkan oleh perangkat WorkSpaces Thin

Client Anda. Anda dapat memantau metrik ini menggunakan CloudWatch konsol, antarmuka baris CloudWatch perintah, atau menggunakan API secara terprogram. CloudWatch juga memungkinkan Anda untuk mengatur alarm ketika Anda mencapai ambang batas yang ditentukan untuk metrik.

Untuk informasi selengkapnya tentang penggunaan CloudWatch dan alarm, lihat [Panduan CloudWatch Pengguna Amazon](#).

Prasyarat

Tidak ada prasyarat. Setelah perangkat WorkSpaces Thin Client terdaftar ke Lingkungan, perangkat akan mulai memancarkan metrik perangkat.

Daftar Isi

- [WorkSpaces Metrik Klien Tipis](#)

WorkSpaces Metrik Klien Tipis

Namespace `AWS/WorkSpacesThinClient` mencakup metrik berikut.

Metrik	Deskripsi	Dimensi	Statistik	Unit
DeviceSession	Jumlah ThinClient perangkat yang terhubung ke sesi perangkat, atau yang tidak dalam sesi.	DesktopType	Rata-rata, Min, Maks, Jumlah, Jumlah Sampel	Hitungan
Connected Devices	Jumlah ThinClient perangkat yang saat ini online.	T/A	Rata-rata, Min, Maks, Jumlah, Jumlah Sampel	Hitungan
SoftwareSetVersion	Jumlah ThinClient perangkat yang	softwareSetVersion	Rata-rata, Min, Maks, Jumlah, Jumlah Sampel	Hitungan

Metrik	Deskripsi	Dimensi	Statistik	Unit
	menjalankan versi Set Perangkat Lunak tertentu.			
NetworkConnectionEthernet	Jumlah ThinClient perangkat yang saat ini terhubung melalui Ethernet.	T/A	Rata-rata, Min, Maks, Jumlah, Jumlah Sampel	Hitungan
NetworkConnectionWifi	Jumlah ThinClient perangkat yang saat ini terhubung melalui WiFi.	T/A	Rata-rata, Min, Maks, Jumlah, Jumlah Sampel	Hitungan

Dimensi ke metrik Klien WorkSpaces Tipis

Dimensi	Deskripsi
DesktopType	Memfilter data metrik menurut jenis desktop yang saat ini sedang dalam sesi di perangkat . Perangkat sedang dalam sesi jika pengguna masuk ke desktop, dan jika perangkat tidak tidur. Jika perangkat dalam sesi, nilai dimensi akan menjadi tipe desktop yang digunakan, seperti WorkSpaces, WorkSpacesSecureBrowser, atau AppStream. Jika perangkat tidak dalam sesi, nilai dimensi akan menjadi NotInSession.

Dimensi	Deskripsi
softwareSetVersion	Memfilter data metrik menurut versi Set Perangkat Lunak yang diinstal pada perangkat. Bentuk dimensi di X.Y.Z, misalnya 1.4.2.

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 CloudFormation ketentuan serta mengonfigurasi sumber daya tersebut untuk Anda.

Bila Anda menggunakan 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 CloudFormation template

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

WorkSpaces Thin Client mendukung pembuatan Lingkungan di 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 CloudFormation

Untuk mempelajari selengkapnya CloudFormation, lihat sumber daya berikut:

- [AWS CloudFormation](#)
- [AWS CloudFormation Panduan Pengguna](#)
- [Referensi 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. 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.

Ubah	Deskripsi	Date
AWS kebijakan terkelola : AmazonWorkSpacesThinClientMonitoringServiceRolePolicy	Amazon WorkSpaces Thin Client menghapus AmazonWorkSpacesThinClientMonitoringServiceRolePolicy bagian.	November 12, 2025
AWS kebijakan terkelola : AmazonWorkSpacesThinClientMonitoringServiceRolePolicy AWS kebijakan terkelola : AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client menambahkan kebijakan AmazonWorkSpacesThinClientMonitoringServiceRolePolicy terkelola. Amazon WorkSpaces Thin Client menambahkan kebijakan AmazonWorkSpacesThinClientFullAccess terkelola versi 3.	26 Agustus 2025
AWS kebijakan terkelola : AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client menambahkan kebijakan AmazonWorkSpacesThinClientFullAccess terkelola versi 2.	Januari 9, 2025
AWS kebijakan terkelola : AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client menambahkan kebijakan AmazonWorkSpacesThinClientR	Januari 9, 2025

Ubah	Deskripsi	Date
	ReadOnlyAccess terkelola versi 3.	
Mencatat panggilan Amazon WorkSpaces Thin Client API menggunakan AWS CloudTrail Pengaturan perangkat Enkripsi data saat istirahat untuk Amazon WorkSpaces Thin Client	Ditambahkan bagian baru untuk peristiwa data. Menambahkan bagian baru untuk pengaturan perangkat. Memperbarui informasi KMS di bagian untuk enkripsi data saat istirahat.	Oktober 28, 2024
Kelangsungan bisnis	Menambahkan bagian baru untuk kelangsungan Bisnis dan pemulihan bencana.	September 6, 2024
AWS kebijakan terkelola : AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client menambahkan kebijakan AmazonWorkSpacesThinClientFullAccess terkelola.	Agustus 9, 2024
AWS kebijakan terkelola : AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client menambahkan kebijakan AmazonWorkSpacesThinClientReadOnlyAccess terkelola versi 2.	Agustus 9, 2024
Mengkonfigurasi WorkSpaces Pribadi untuk Klien WorkSpaces Tipis	Memperbarui untuk WorkSpaces Pribadi baru.	Agustus 7, 2024

Ubah	Deskripsi	Date
Mengkonfigurasi WorkSpaces Kolam untuk Klien WorkSpaces Tipis	Menambahkan bagian baru untuk WorkSpaces Pools baru.	Agustus 7, 2024
AWS kebijakan terkelola : AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client menambahkan kebijakan AmazonWorkSpacesThinClientReadOnlyAccess terkelola.	Juli 19, 2024
AWS kebijakan terkelola untuk Amazon WorkSpaces Thin Client	Amazon WorkSpaces Thin Client mulai melacak perubahan.	Juli 19, 2024
Mengkonfigurasi WorkSpaces untuk Amazon WorkSpaces Thin Client	Memperbarui daftar sistem operasi.	Februari 12, 2024
Mengkonfigurasi WorkSpaces Aplikasi untuk Amazon WorkSpaces Thin Client	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.