aws

Panduan Administrasi

Amazon WorkSpaces

Amazon WorkSpaces: Panduan Administrasi

Table of Contents

Apa itu Amazon WorkSpaces?

Amazon WorkSpaces memungkinkan Anda menyediakan desktop Microsoft Windows, Amazon Linux, atau Ubuntu Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai. WorkSpaces WorkSpaces menghilangkan kebutuhan untuk mendapatkan dan menyebarkan perangkat keras atau menginstal perangkat lunak yang kompleks. Anda dapat dengan cepat menambahkan atau menghapus pengguna saat kebutuhan Anda berubah. Pengguna dapat mengakses desktop virtual mereka dari beberapa perangkat atau peramban web.

Untuk informasi lebih lanjut, lihat Amazon WorkSpaces.

Fitur

- Pilih sistem operasi Anda (Windows, Amazon Linux, Ubuntu Linux) dan pilih dari berbagai konfigurasi perangkat keras, konfigurasi perangkat lunak, dan AWS Wilayah. Untuk informasi selengkapnya, lihat Amazon WorkSpaces Bundles danthe section called “Buat citra dan paket kustom”.
- Pilih protokol Anda: PCoIP atau WorkSpaces Streaming Protocol (WSP). Untuk informasi selengkapnya, lihat Protokol untuk Amazon WorkSpaces.
- Connect ke Anda WorkSpace dan ambil dari kanan di mana Anda tinggalkan. WorkSpacesmemberikan pengalaman desktop yang persisten.
- WorkSpaces memberikan fleksibilitas baik tagihan bulanan atau per jam untuk. WorkSpaces Untuk informasi lebih lanjut, lihat WorkSpaces Harga.
- Untuk desktop Windows, Anda dapat membawa lisensi dan aplikasi Anda sendiri, atau membelinya dari AWS Marketplace untuk Aplikasi Desktop.
- Buat direktori terkelola mandiri untuk pengguna Anda, atau sambungkan WorkSpaces ke direktori lokal sehingga pengguna dapat menggunakan kredensialnya yang ada untuk mendapatkan akses tanpa batas ke sumber daya perusahaan. Untuk informasi selengkapnya, lihat Direktori.
- Gunakan alat yang sama untuk mengelola WorkSpaces yang Anda gunakan untuk mengelola desktop lokal.
- Gunakan autentikasi multi-factor (MFA) untuk keamanan tambahan.
- Gunakan AWS Key Management Service (AWS KMS) untuk mengenkripsi data at rest, disk I/O, dan snapshot volume.
- Kontrol alamat IP dari mana pengguna diizinkan untuk mengakses mereka WorkSpaces.

Arsitektur

Untuk Windows dan Linux WorkSpaces, masing-masing WorkSpace dikaitkan dengan virtual private cloud (VPC), dan direktori untuk menyimpan dan mengelola informasi untuk Anda WorkSpaces dan pengguna. Untuk informasi selengkapnya, lihat the section called “Persyaratan VPC”. Direktori dikelola melalui AWS Directory Service, yang menawarkan pilihan berikut: Simple AD, AD Connector, atau AWS Directory Service for Direktori Aktif Microsoft, juga dikenal sebagai Microsoft AD Terkelola AWS. Untuk informasi selengkapnya, lihat Panduan Administrasi AWS Directory Service.

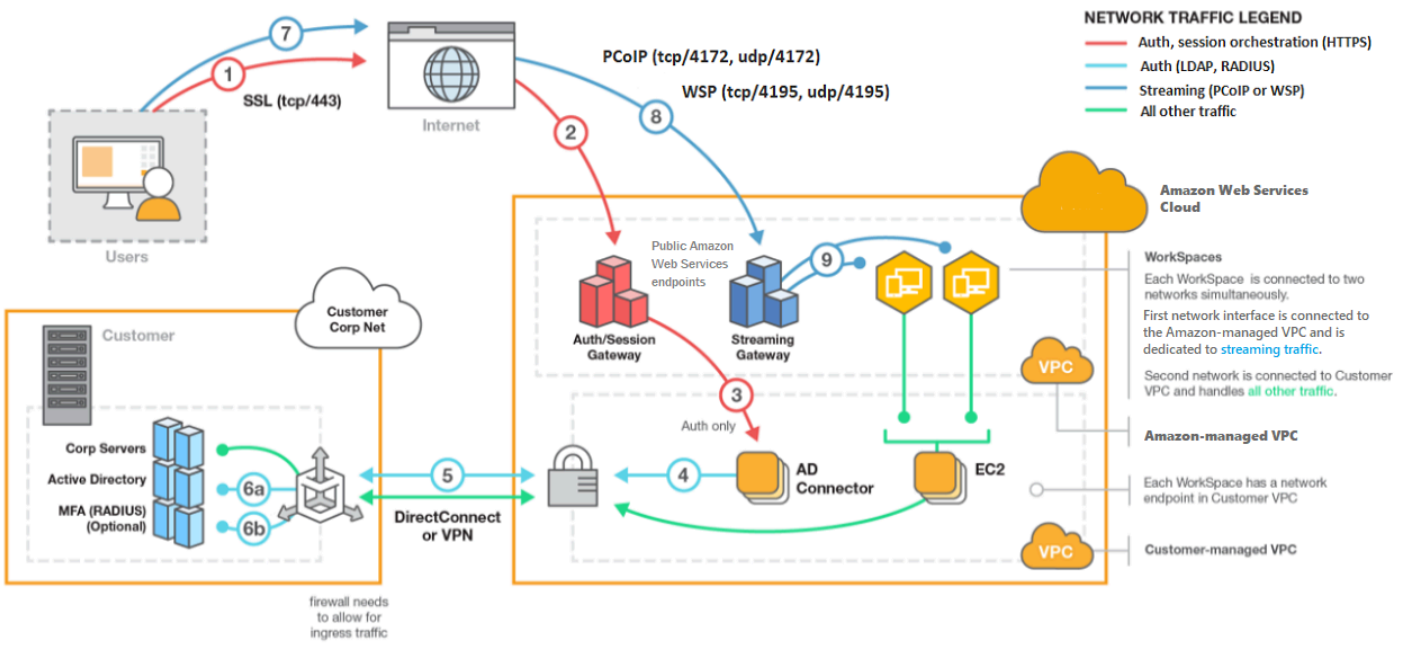
WorkSpaces menggunakan direktori Simple AD, AD Connector, atau AWS Managed Microsoft AD untuk mengautentikasi pengguna. Pengguna mengakses mereka WorkSpaces dengan menggunakan aplikasi klien dari perangkat yang didukung atau, untuk Windows WorkSpaces, browser web, dan mereka masuk dengan menggunakan kredensi direktori mereka. Informasi login dikirim ke gateway otentikasi, yang meneruskan lalu lintas ke direktori untuk. WorkSpace Setelah pengguna diautentikasi, lalu lintas streaming dimulai melalui gateway streaming.

Aplikasi klien menggunakan HTTPS melalui port 443 untuk semua autentikasi dan informasi terkait sesi. Aplikasi klien menggunakan port 4172 (PCoIP) dan port 4195 (WSP) untuk streaming piksel ke dan port 4172 WorkSpace dan 4195 untuk pemeriksaan kesehatan jaringan. Untuk informasi selengkapnya, lihat Port untuk aplikasi klien.

Masing-masing WorkSpace memiliki dua antarmuka jaringan elastis yang terkait dengannya: antarmuka jaringan untuk manajemen dan streaming (eth0) dan antarmuka jaringan utama (eth1). Antarmuka jaringan utama memiliki alamat IP yang diberikan oleh VPC Anda, dari subnet yang sama yang digunakan oleh direktori. Ini memastikan bahwa lalu lintas dari Anda WorkSpace dapat dengan mudah mencapai direktori. Akses ke sumber daya di VPC dikendalikan oleh grup keamanan yang ditetapkan ke antarmuka jaringan utama. Untuk informasi selengkapnya, lihat Antarmuka jaringan.

Diagram berikut menunjukkan arsitektur WorkSpaces.

Amazon WorkSpaces Architectural Diagram



Akses Anda WorkSpace

Anda dapat terhubung ke Anda WorkSpaces dengan menggunakan aplikasi klien untuk perangkat yang didukung dengan menggunakan browser web yang didukung pada sistem operasi yang didukung.

> **Note**
>
> Anda tidak dapat menggunakan browser web untuk terhubung ke Amazon Linux WorkSpaces.

Terdapat aplikasi klien untuk perangkat berikut:

- Komputer Windows
- Komputer macOS
- Komputer Ubuntu Linux 18.04
- Chromebook
- iPad

- Perangkat android
- Tablet fire
- Perangkat nol klien (Perangkat klien nol Teradici hanya didukung dengan PCoIP.)

Pada PC Windows, macOS, dan Linux, Anda dapat menggunakan browser web berikut untuk terhubung ke Windows dan Ubuntu Linux: WorkSpaces

- Chrome 53 dan yang lebih baru (hanya Windows dan macOS)
- Firefox 49 dan yang lebih baru

Untuk informasi selengkapnya, lihat WorkSpaces Klien di Panduan WorkSpaces Pengguna Amazon.

Harga

Setelah Anda mendaftarAWS, Anda dapat memulai dengan WorkSpaces gratis menggunakan penawaran tingkat WorkSpaces gratis. Untuk informasi lebih lanjut, lihat WorkSpaces Harga.

Dengan WorkSpaces, Anda hanya membayar untuk apa yang Anda gunakan. Anda dikenakan biaya berdasarkan bundel dan jumlah WorkSpaces yang Anda luncurkan. Harga untuk WorkSpaces mencakup penggunaan Simple AD dan AD Connector tetapi tidak menggunakan AWS Managed Microsoft AD.

WorkSpaces menyediakan tagihan bulanan atau per jam untuk. WorkSpaces Dengan penagihan bulanan, Anda membayar biaya tetap untuk penggunaan tak terbatas, yang terbaik untuk pengguna yang menggunakan waktu WorkSpaces penuh mereka. Dengan penagihan per jam, Anda membayar biaya bulanan tetap kecil per WorkSpace, ditambah tarif per jam yang rendah untuk setiap jam yang sedang berjalan. WorkSpace Untuk informasi lebih lanjut, lihat WorkSpaces Harga.

Untuk informasi tentang wilayah yang didukung, lihat WorkSpaces Harga.

Cara memulai

Untuk membuat WorkSpace, coba salah satu tutorial berikut:

- Memulai dengan penyiapan WorkSpaces cepat
- Luncurkan WorkSpace menggunakan Microsoft AD yang AWS Dikelola
- Luncurkan WorkSpace menggunakan Simple AD

- Luncurkan WorkSpace menggunakan AD Connector
- Luncurkan WorkSpace menggunakan domain tepercaya

Anda mungkin juga ingin menjelajahi sumber daya ini untuk mempelajari lebih lanjut tentang Amazon WorkSpaces:

- Menyediakan Desktop di Cloud
- Praktik Terbaik untuk Menyebarkan Amazon WorkSpaces
- WorkSpaces Sumber daya Amazon - termasuk whitepaper, posting blog, webinar, dan sesi re:Invent
- Amazon WorkSpaces FAQ

Memulai dengan penyiapan WorkSpaces cepat

Dalam tutorial ini, Anda mempelajari cara menyediakan desktop Microsoft Windows, Amazon Linux, atau Ubuntu Linux virtual berbasis cloud, yang dikenal sebagai WorkSpace, dengan menggunakan WorkSpaces dan. AWS Directory Service

Tutorial ini menggunakan opsi pengaturan cepat untuk meluncurkan Anda WorkSpace. Opsi ini hanya tersedia jika Anda belum pernah meluncurkan file WorkSpace. Alternatif lainnya, lihat Luncurkan desktop virtual menggunakan WorkSpaces.

> **Note**
>
> Pengaturan cepat didukung di AWS Wilayah berikut:
>
> - US East (N. Virginia)
> - US West (Oregon)
> - Europe (Ireland)
> - Asia Pacific (Singapore)
> - Asia Pacific (Sydney)
> - Asia Pacific (Tokyo)
>
> Untuk mengubah Wilayah Anda, lihat Memilih Wilayah.

Tugas

Sebelum Anda memulai

Sebelum Anda memulai, pastikan Anda memenuhi persyaratan berikut:

- Anda harus memiliki AWS akun untuk membuat atau mengelola. WorkSpace Pengguna tidak memerlukan AWS akun untuk terhubung dan menggunakannya WorkSpaces.
- WorkSpaces tidak tersedia di setiap wilayah. Verifikasi Wilayah yang didukung dan pilih Wilayah untuk Anda WorkSpaces. Untuk informasi selengkapnya tentang Wilayah yang didukung, lihat WorkSpaces Harga menurut AWS Wilayah.

Ini juga membantu untuk meninjau dan memahami hal-hal berikut sebelum Anda melanjutkan:

- Saat Anda meluncurkan WorkSpace, Anda harus memilih WorkSpace bundel. Untuk informasi selengkapnya, lihat WorkSpaces Paket Amazon dan WorkSpaces Harga Amazon.
- Ketika Anda meluncurkan WorkSpace, Anda harus memilih protokol (PCoIP atau WorkSpaces Streaming Protocol [WSP]) yang ingin Anda gunakan dengan bundel Anda. Untuk informasi selengkapnya, lihat Protokol untuk Amazon WorkSpaces.
- Ketika Anda meluncurkan WorkSpace, Anda harus menentukan informasi profil untuk pengguna, termasuk nama pengguna dan alamat email. Pengguna melengkapi profil mereka dengan menentukan kata sandi. Informasi tentang WorkSpaces dan pengguna disimpan dalam direktori. Untuk informasi selengkapnya, lihat Direktori.

Apa yang dilakukan pengaturan cepat

Penyiapan cepat menyelesaikan tugas-tugas berikut atas nama Anda:

- Membuat peran IAM untuk memungkinkan WorkSpaces layanan membuat antarmuka jaringan elastis dan daftar direktori Anda WorkSpaces . Peran ini memiliki nama `workspaces_DefaultRole`.
- Membuat virtual private cloud (VPC). Jika Anda ingin menggunakan VPC yang sudah ada, pastikan VPC tersebut memenuhi persyaratan yang disebutkan dalam Konfigurasikan VPC untuk WorkSpaces, lalu ikuti langkah-langkah di salah satu tutorial yang terdaftar di Luncurkan desktop virtual menggunakan WorkSpaces. Pilih tutorial yang sesuai dengan tipe Direktori Aktif yang ingin Anda gunakan.
- Menyiapkan direktori Simple AD di VPC dan mengaktifkannya untuk Amazon. WorkDocs Direktori Simple AD ini digunakan untuk menyimpan pengguna dan WorkSpace informasi. Yang pertama

Akun AWS dibuat oleh pengaturan cepat adalah admin AndaAkun AWS. † Direktori ini juga memiliki akun Administrator. Untuk informasi selengkapnya, lihat Apa yang dibuat di Panduan AWS Directory Service Administrasi.

- Membuat yang ditentukan Akun AWS dan menambahkannya ke direktori.
- Menciptakan WorkSpaces. Masing-masing WorkSpace menerima alamat IP publik untuk menyediakan akses internet. Mode berjalan adalah AlwaysOn. Untuk informasi selengkapnya, lihat Kelola mode WorkSpace berjalan.
- Mengirim email undangan ke pengguna tertentu. Jika pengguna Anda tidak menerima email undangan, lihat Kirim email undangan.

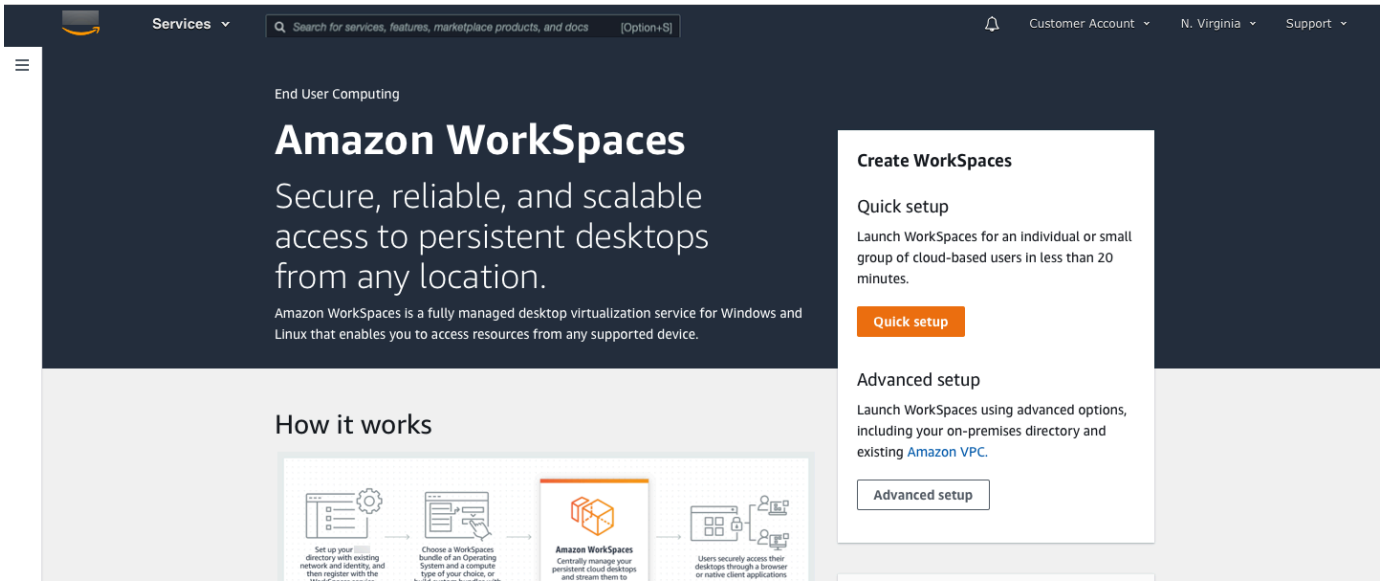
† Yang pertama Akun AWS dibuat oleh pengaturan cepat adalah admin AndaAkun AWS. Anda tidak dapat memperbarui ini Akun AWS dari WorkSpaces Konsol. Jangan berbagi informasi untuk akun ini dengan orang lain. Untuk mengundang pengguna lain untuk menggunakan WorkSpaces, buat yang baru Akun AWS untuk mereka.

Langkah 1: Luncurkan WorkSpace

Menggunakan pengaturan cepat, Anda dapat meluncurkan yang pertama WorkSpace dalam hitungan menit.

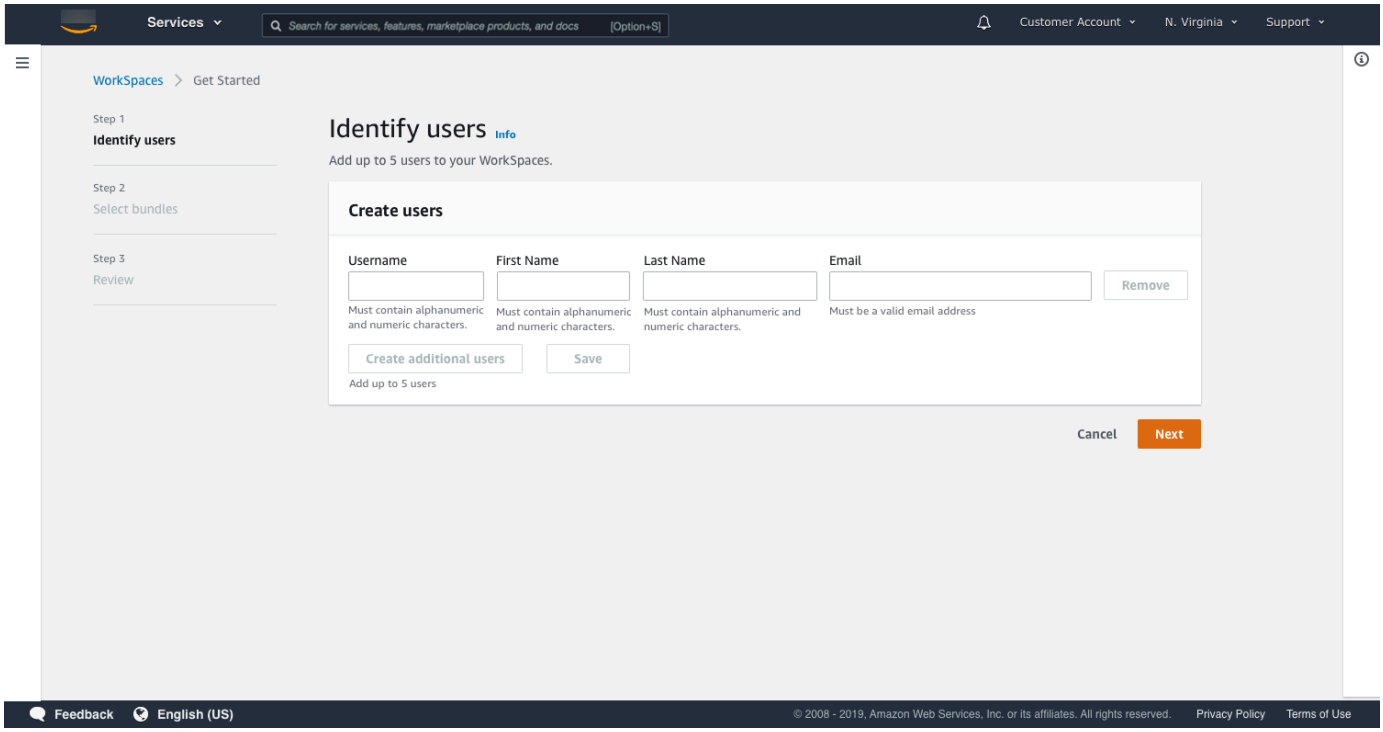
Untuk meluncurkan WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Pilih Pengaturan cepat. Jika Anda tidak melihat tombol ini, Anda telah meluncurkan WorkSpace di Wilayah ini, atau Anda tidak menggunakan salah satu Wilayah yang mendukung penyiapan cepat. Dalam hal ini, lihat Luncurkan desktop virtual menggunakan WorkSpaces.

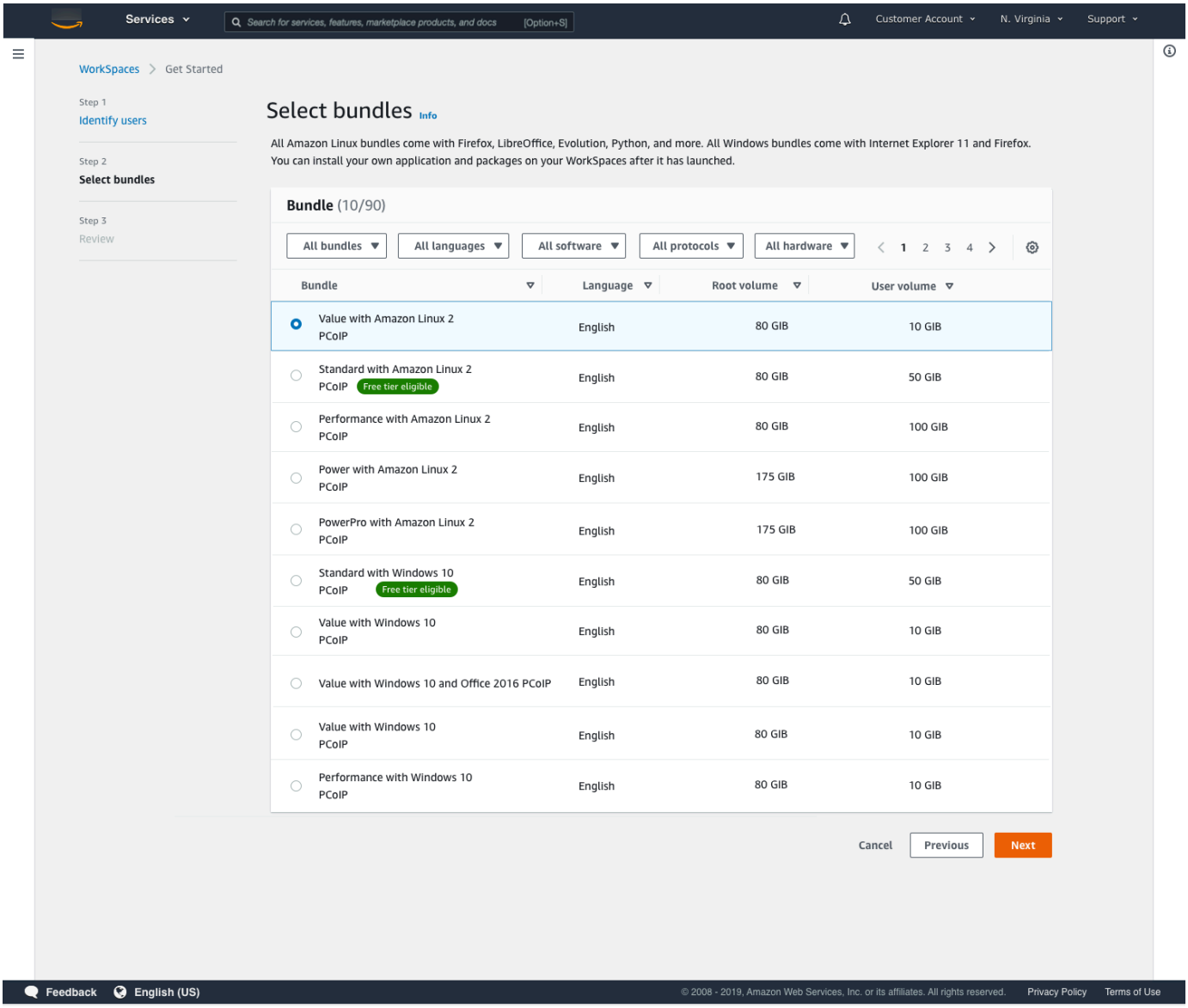


3. Untuk Identifikasi pengguna, masukkan Nama Pengguna, Nama Depan. Nama Belakang, dan Email. Kemudian pilih Selanjutnya.

> **Note**
>
> Jika ini adalah pertama kalinya Anda menggunakan WorkSpaces, kami sarankan membuat pengguna untuk diri Anda sendiri untuk tujuan pengujian.



4. Untuk Paket, pilih paket (perangkat keras dan perangkat lunak) untuk pengguna dengan protokol yang sesuai (PCoIP atau WSP). Untuk informasi selengkapnya tentang berbagai bundel publik yang tersedia untuk Amazon WorkSpaces, lihat Amazon WorkSpaces Bundles.



5. Tinjau informasi Anda. Lalu pilih Buat WorkSpace.
6. Dibutuhkan sekitar 20 menit WorkSpace untuk Anda meluncurkannya. Untuk memantau kemajuan, buka panel navigasi sebelah kiri dan pilih Direktori. Anda akan melihat direktori yang dibuat dengan status awal `REQUESTED` lalu `CREATING`.

   Setelah direktori dibuat dan memiliki status`ACTIVE`, Anda dapat memilih WorkSpacesdi panel navigasi kiri untuk memantau kemajuan proses WorkSpace peluncuran. Status awal dari WorkSpace adalah`PENDING`. Saat peluncuran selesai, statusnya adalah `AVAILABLE` dan undangan dikirim ke alamat email yang Anda tentukan untuk setiap pengguna. Jika pengguna Anda tidak menerima email undangan, lihat Kirim email undangan.

Langkah 2: Connect ke WorkSpace

Setelah Anda menerima email undangan, Anda dapat terhubung ke WorkSpace menggunakan klien pilihan Anda. Setelah Anda masuk, klien akan menampilkan WorkSpace desktop.

Untuk terhubung ke WorkSpace

1. Jika Anda belum menyiapkan kredensial untuk pengguna, buka tautan di email undangan dan ikuti petunjuknya. Ingat kata sandi yang Anda tentukan karena Anda akan membutuhkannya untuk terhubung ke Anda WorkSpace.

   > **Note**
   >
   > Kata sandi peka terhadap huruf besar-kecil dan harus antara 8 hingga 64 karakter, inklusif. Kata sandi harus berisi setidaknya satu karakter dari masing-masing kategori berikut: huruf kecil (a-z), huruf besar (A-Z), angka (0-9), dan set karakter ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Tinjau WorkSpaces Klien di Panduan WorkSpaces Pengguna Amazon untuk informasi selengkapnya tentang persyaratan untuk setiap klien, lalu lakukan salah satu hal berikut:

   - Saat diminta, unduh salah satu aplikasi client atau luncurkan Akses Web.
   - Jika Anda tidak diminta dan Anda belum menginstal aplikasi klien, buka https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

   > **Note**
   >
   > Anda tidak dapat menggunakan browser web (Akses Web) untuk terhubung ke Amazon Linux WorkSpaces.

3. Mulai client, masukkan kode pendaftaran dari email undangan, dan pilih Daftar.
4. Saat diminta untuk masuk, masukkan kredenal masuk, lalu pilih Masuk.
5. (Opsional) Saat diminta untuk menyimpan kredensial Anda, pilih Ya.

Untuk informasi selengkapnya tentang penggunaan aplikasi klien, seperti menyiapkan beberapa monitor atau menggunakan perangkat periferal, lihat Dukungan WorkSpaces Klien dan Perangkat Periferal di Panduan WorkSpaces Pengguna Amazon.

Langkah 3: (Opsional) Bersihkan

Jika Anda selesai dengan WorkSpace yang Anda buat untuk tutorial ini, Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat the section called “Menghapus WorkSpace”.

> **Note**
>
> Simple AD tersedia untuk Anda secara gratis untuk digunakan WorkSpaces. Jika tidak ada yang WorkSpaces digunakan dengan direktori Simple AD Anda selama 30 hari berturut-turut, direktori ini akan secara otomatis dideregistrasi untuk digunakan dengan Amazon WorkSpaces, dan Anda akan dikenakan biaya untuk direktori ini sesuai ketentuan harga. AWS Directory Service
>
> Untuk menghapus direktori kosong, lihat Hapus direktori untuk WorkSpaces. Jika Anda menghapus direktori Simple AD Anda, Anda selalu dapat membuat yang baru ketika Anda ingin mulai menggunakan WorkSpaces lagi.

Langkah selanjutnya

Anda dapat terus menyesuaikan WorkSpace yang baru saja Anda buat. Misalnya, Anda dapat menginstal perangkat lunak dan kemudian membuat bundel khusus dari Anda WorkSpace. Anda juga dapat melakukan berbagai tugas administratif untuk WorkSpaces direktori Anda WorkSpaces dan Anda. Untuk informasi selengkapnya, lihat dokumentasi berikut.

- Buat WorkSpaces gambar dan bundel khusus
- Kelola Anda WorkSpaces
- Kelola direktori untuk WorkSpaces

Untuk membuat tambahan WorkSpaces, lakukan salah satu hal berikut:

- Jika Anda ingin terus menggunakan VPC dan direktori Simple AD yang dibuat dengan pengaturan cepat, Anda dapat menambahkan WorkSpaces untuk pengguna tambahan dengan mengikuti langkah-langkah di Langkah 2: Buat WorkSpace bagian Launch a WorkSpace Using Simple AD tutorial.
- Jika Anda perlu menggunakan tipe direktori lain atau jika Anda perlu menggunakan Direktori Aktif yang sudah ada, lihat tutorial yang sesuai di Luncurkan desktop virtual menggunakan WorkSpaces.

Untuk informasi selengkapnya tentang penggunaan aplikasi WorkSpaces klien, seperti menyiapkan beberapa monitor atau menggunakan perangkat periferal, lihat Dukungan WorkSpaces Klien dan Perangkat Periferal di Panduan WorkSpaces Pengguna Amazon.

Memulai dengan penyiapan WorkSpaces lanjutan

Dalam tutorial ini, Anda mempelajari cara menyediakan desktop Microsoft Windows atau Amazon Linux virtual berbasis cloud, yang dikenal sebagai WorkSpace, dengan menggunakan WorkSpaces dan. AWS Directory Service

Tutorial ini menggunakan opsi pengaturan lanjutan untuk meluncurkan Anda WorkSpace.

> **Note**
>
> Pengaturan lanjutan didukung di semua Wilayah untuk WorkSpaces.

Tugas

- Sebelum Anda memulai
- Menggunakan pengaturan lanjutan untuk meluncurkan WorkSpace

Sebelum Anda memulai

Sebelum memulai, pastikan Anda memiliki AWS akun yang dapat Anda gunakan untuk membuat atau mengelola akun. WorkSpace Pengguna tidak memerlukan AWS akun untuk terhubung dan menggunakannya WorkSpaces.

Tinjau dan pahami konsep-konsep berikut sebelum Anda melanjutkan:

- Saat Anda meluncurkan WorkSpace, Anda harus memilih WorkSpace bundel. Untuk informasi selengkapnya, lihat Amazon WorkSpaces Bundles.
- Ketika Anda meluncurkan WorkSpace, Anda harus memilih protokol (PCoIP atau WorkSpaces Streaming Protocol [WSP]) yang ingin Anda gunakan dengan bundel Anda. Untuk informasi selengkapnya, lihat Protokol untuk Amazon WorkSpaces.
- Ketika Anda meluncurkan WorkSpace, Anda harus menentukan informasi profil untuk pengguna, termasuk nama pengguna dan alamat email. Pengguna melengkapi profil mereka dengan menentukan kata sandi. Informasi tentang WorkSpaces dan pengguna disimpan dalam direktori. Untuk informasi selengkapnya, lihat Direktori.

Menggunakan pengaturan lanjutan untuk meluncurkan WorkSpace

Untuk menggunakan pengaturan lanjutan untuk meluncurkan WorkSpace:

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Pilih salah satu jenis direktori berikut, lalu pilih Berikutnya:
   - Microsoft AD yang Dikelola AWS
   - Simple AD
   - AD Connector
3. Masukkan informasi direktori.
4. Pilih dua subnet dalam VPC dari dua zona ketersediaan yang berbeda. Untuk informasi selengkapnya, lihat Mengkonfigurasi VPC dengan subnet publik.
5. Tinjau informasi direktori Anda dan pilih Buat direktori.

Jaringan dan akses untuk WorkSpaces

Sebagai WorkSpace administrator, Anda harus memahami hal-hal berikut tentang WorkSpaces jaringan dan akses.

Konten

Protokol untuk Amazon WorkSpaces

Amazon WorkSpaces mendukung dua protokol: PCoIP dan WorkSpaces Streaming Protocol (WSP). Protokol yang Anda pilih bergantung pada beberapa faktor, seperti jenis perangkat yang akan diakses pengguna Anda, sistem operasi mana yang ada di Anda WorkSpaces, kondisi jaringan apa yang akan dihadapi pengguna Anda, dan apakah pengguna Anda memerlukan dukungan video dua arah. WorkSpaces

Persyaratan

WSP hanya WorkSpaces didukung dengan persyaratan minimum berikut.

Persyaratan agen tuan rumah:

- Agen host Windows versi 2.0.0.312 atau lebih tinggi
- Agen host Ubuntu versi 2.1.0.501 atau lebih tinggi
- Agen host Amazon Linux 2 versi 2.0.0.596 atau lebih tinggi

Persyaratan klien:

- Versi klien asli Windows 5.1.0.329 atau lebih tinggi
- klien asli macOS versi 5.5.0 atau lebih tinggi
- Akses Web

Untuk informasi selengkapnya tentang cara memeriksa versi WorkSpace klien dan versi agen host Anda, lihat FAQ.

Waktu saat harus menggunakan WSP

- Jika Anda memerlukan toleransi kerugian/latensi yang lebih tinggi untuk mendukung kondisi jaringan pengguna akhir Anda. Misalnya, Anda memiliki pengguna yang mengakses jarak WorkSpaces global mereka atau menggunakan jaringan yang tidak dapat diandalkan.
- Jika Anda memerlukan pengguna untuk mengautentikasi dengan kartu pintar atau menggunakan kartu pintar dalam sesi.
- Jika Anda membutuhkan kemampuan dukungan webcam dalam sesi.
- Jika Anda perlu menggunakan Akses Web dengan WorkSpaces bundel bertenaga Windows Server 2019.
- Jika Anda perlu menggunakan Ubuntu WorkSpaces.
- Jika Anda perlu menggunakan Windows 11 BYOL WorkSpaces.
- Jika Anda perlu menggunakan bundel berbasis GPU Ubuntu (Graphics.g4dn dan.g4dn). GraphicsPro
- Jika Anda membutuhkan pengguna untuk mengautentikasi dalam sesi dengan WebAuthn autentikator seperti YubiKey atau Windows Hello.

Waktu ketika harus menggunakan PCoIP

- Jika Anda ingin menggunakan klien iPad atau Android Linux.
- Jika Anda menggunakan perangkat client zero Teradici.
- Jika Anda perlu menggunakan bundel berbasis GPU (Graphics.g4dn, .g4dn, Graphics, atau). GraphicsPro GraphicsPro
- Jika Anda perlu menggunakan paket Linux untuk kasus penggunaan kartu non-pintar.
- Jika Anda perlu menggunakan WorkSpaces di Wilayah China (Ningxia).

> **Note**
>
> - Sebuah direktori dapat memiliki campuran PCoIP dan WSP WorkSpaces di dalamnya.
> - Seorang pengguna dapat memiliki PCoIP dan WSP WorkSpace selama keduanya WorkSpaces berada di direktori terpisah. Pengguna yang sama tidak dapat memiliki PCoIP dan WSP WorkSpace di direktori yang sama. Untuk informasi selengkapnya tentang membuat beberapa WorkSpaces untuk pengguna, lihatBuat beberapa WorkSpaces untuk pengguna.
> - Anda dapat memigrasikan WorkSpace antara dua protokol dengan menggunakan fitur WorkSpaces migrasi, yang memerlukan pembuatan ulang protokol. WorkSpace Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.
> - Jika Anda WorkSpace dibuat dengan bundel PCoIP, Anda dapat memodifikasi protokol streaming untuk bermigrasi di antara dua protokol tanpa memerlukan pembangunan kembali, sambil mempertahankan volume root. Untuk informasi selengkapnya, lihat Memodifikasi protokol.
> - Untuk pengalaman terbaik dengan konferensi video, kami sarankan menggunakan Power atau PowerPro bundel saja.

Konfigurasikan VPC untuk WorkSpaces

WorkSpaces meluncurkan Anda WorkSpaces di cloud pribadi virtual (VPC).

Anda dapat membuat VPC dengan dua subnet pribadi untuk Anda WorkSpaces dan gateway NAT di subnet publik. Atau, Anda dapat membuat VPC dengan dua subnet publik untuk Anda WorkSpaces dan mengaitkan alamat IP publik atau alamat IP Elastis dengan masing-masing subnet. WorkSpace

Untuk informasi selengkapnya tentang pertimbangan desain VPC, lihat Praktik Terbaik untuk VPC dan Jaringan di WorkSpaces Penerapan Amazon dan Praktik Terbaik untuk Penerapan - Desain VPC. WorkSpaces

Daftar Isi

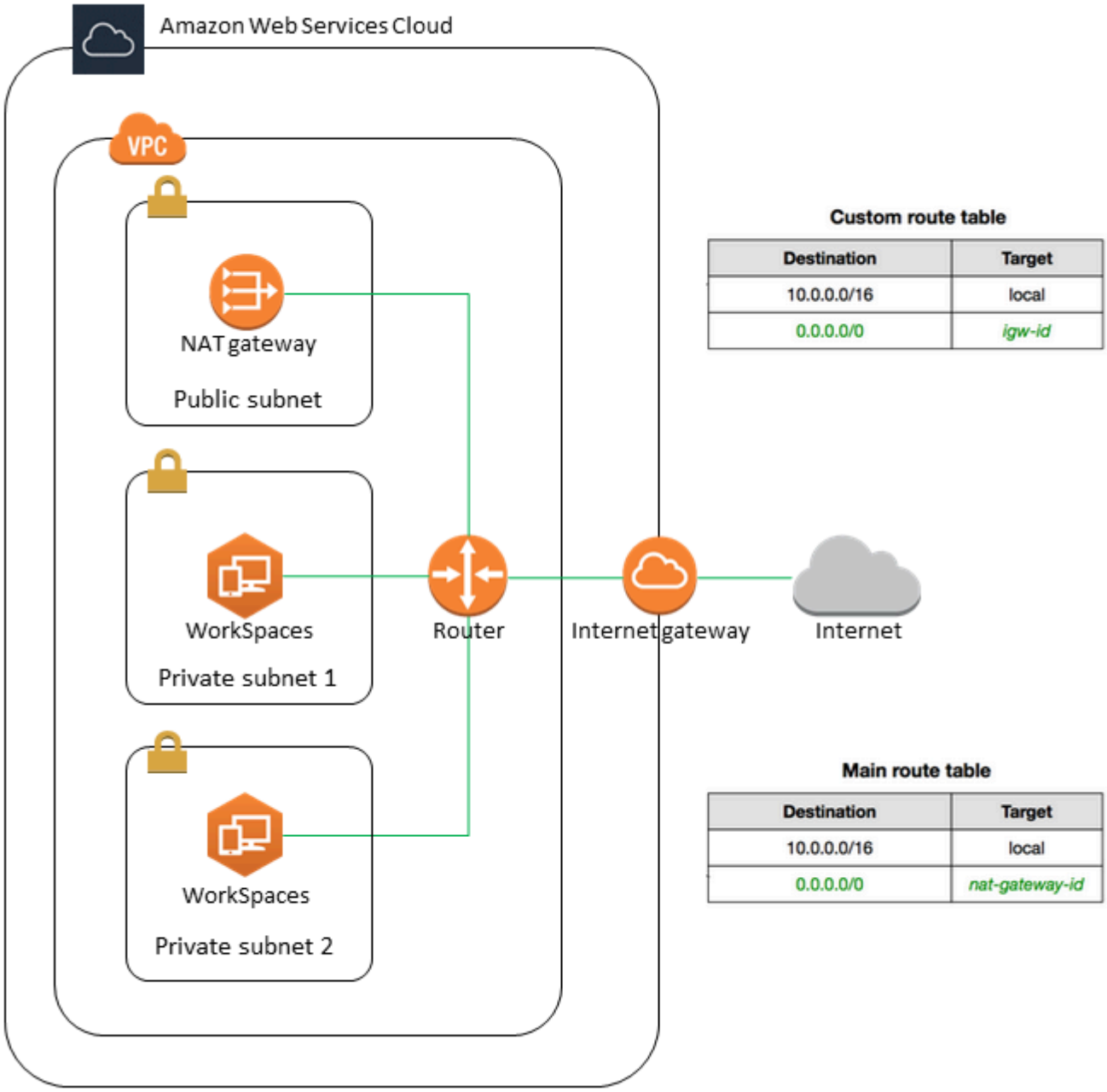
Persyaratan

Subnet VPC Anda harus berada di Availability Zone yang berbeda di Wilayah tempat Anda meluncurkan. WorkSpaces Availability Zone berada di lokasi yang berjauhan yang ditata sedemikian rupa agar terisolasi dari kegagalan Availability Zone lain. Dengan meluncurkan instans dalam Availability Zone yang terpisah, Anda dapat melindungi aplikasi Anda dari kegagalan di satu lokasi. Setiap subnet harus berada sepenuhnya dalam satu Availability Zone dan tidak dapat memperluas zona.

> **Note**
>
> Amazon WorkSpaces tersedia dalam subset Availability Zones di setiap Wilayah yang didukung. Untuk menentukan Availability Zone yang dapat Anda gunakan untuk subnet VPC yang Anda gunakan WorkSpaces, lihat. Zona Ketersediaan untuk Amazon WorkSpaces

Konfigurasi VPC dengan subnet privat dan gateway NAT

Jika Anda menggunakan AWS Directory Service untuk membuat Microsoft yang Dikelola AWS atau Simple AD, sebaiknya Anda mengonfigurasi VPC dengan satu subnet publik dan dua subnet privat. Konfigurasikan direktori Anda WorkSpaces untuk meluncurkan subnet pribadi Anda. Untuk menyediakan akses internet ke WorkSpaces subnet pribadi, konfigurasikan gateway NAT di subnet publik.



Untuk membuat VPC dengan satu subnet publik dan dua subnet pribadi

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih Buat VPC.
3. Pada Sumber daya yang akan dibuat, pilih VPC dan lainnya.
4. Untuk Pembuatan otomatis tanda nama, masukkan nama untuk VPC.

5. Untuk mengkonfigurasi subnet, lakukan hal berikut:

    a. Untuk Jumlah Availability Zone, pilih 1 atau 2, tergantung kebutuhan Anda.

    b. Perluas Kustomisasi AZ dan pilih Availability Zones Anda. Jika tidak, AWS pilih mereka untuk Anda. Untuk membuat pilihan yang tepat, lihatZona Ketersediaan untuk Amazon WorkSpaces.

    c. Untuk Jumlah subnet publik, pastikan Anda memiliki satu subnet publik per Availability Zone.

    d. Untuk Jumlah subnet pribadi, pastikan Anda memiliki setidaknya satu subnet pribadi per Availability Zone.

    e. Masukkan blok CIDR untuk setiap subnet. Untuk informasi selengkapnya, lihat Ukuran subnet di Panduan Pengguna Amazon VPC.

6. Untuk gateway NAT, pilih 1 per AZ.

7. Pilih Buat VPC.

Blok IPv6 CIDR

Anda dapat mengaitkan blok IPv6 CIDR dengan VPC dan subnet Anda. Namun, jika Anda mengonfigurasi subnet Anda untuk secara otomatis menetapkan alamat IPv6 bagi instans yang diluncurkan di subnet, maka Anda tidak dapat menggunakan paket Graphics. (Namun, Anda dapat menggunakan Graphics.g4dn, GraphicsPro .g4dn, dan bundel.) GraphicsPro Pembatasan ini muncul dari pembatasan perangkat keras tipe instans sebelumnya yang tidak mendukung IPv6.

Untuk mengatasi masalah ini, Anda dapat menonaktifkan sementara pengaturan alamat IPv6 penetapan otomatis pada WorkSpaces subnet sebelum meluncurkan bundel Grafik, dan kemudian mengaktifkan kembali pengaturan ini (jika perlu) setelah meluncurkan bundel Grafik sehingga bundel lain menerima alamat IP yang diinginkan.

Secara default, pengaturan tetapkan alamat IPv6 secara otomatis dinonaktifkan. Untuk memeriksa pengaturan ini dari konsol Amazon VPC, pilih Subnet di panel navigasi. Pilih subnet, lalu pilih Tindakan, Ubah pengaturan penetapan IP otomatis.

Mengonfigurasi VPC dengan subnet publik

Jika mau, Anda bisa membuat VPC dengan dua subnet publik. Untuk menyediakan akses internet ke WorkSpaces subnet publik, konfigurasikan direktori untuk menetapkan alamat IP Elastis secara otomatis atau manual menetapkan alamat IP Elastis ke masing-masing subnet. WorkSpace

Tugas

- Langkah 1: Buat VPC
- Langkah 2: Tetapkan alamat IP publik ke alamat Anda WorkSpaces

Langkah 1: Buat VPC

Buat VPC dengan satu subnet publik seperti berikut.

Untuk membuat VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih Buat VPC.
3. Pada Sumber daya yang akan dibuat, pilih VPC dan lainnya.
4. Untuk Pembuatan otomatis tanda nama, masukkan nama untuk VPC.
5. Untuk mengkonfigurasi subnet, lakukan hal berikut:
    a. Untuk Jumlah Availability Zone, pilih 2.
    b. Perluas Kustomisasi AZ dan pilih Availability Zones Anda. Jika tidak, AWS pilih mereka untuk Anda. Untuk membuat pilihan yang tepat, lihatZona Ketersediaan untuk Amazon WorkSpaces.
    c. Untuk Jumlah subnet publik, pilih 2.
    d. Untuk Jumlah subnet pribadi, pilih 0.
    e. Masukkan blok CIDR untuk setiap subnet publik. Untuk informasi selengkapnya, lihat Ukuran subnet di Panduan Pengguna Amazon VPC.
6. Pilih Buat VPC.

Blok IPv6 CIDR

Anda dapat mengaitkan blok CIDR IPv6 dengan VPC dan subnet Anda. Namun, jika Anda mengonfigurasi subnet Anda untuk secara otomatis menetapkan alamat IPv6 bagi instans yang diluncurkan di subnet, maka Anda tidak dapat menggunakan paket Graphics. (Namun, Anda dapat menggunakan GraphicsPro bundel.) Pembatasan ini muncul dari pembatasan perangkat keras tipe instans sebelumnya yang tidak mendukung IPv6.

Untuk mengatasi masalah ini, Anda dapat menonaktifkan sementara pengaturan alamat IPv6 penetapan otomatis pada WorkSpaces subnet sebelum meluncurkan bundel Grafik, dan kemudian

mengaktifkan kembali pengaturan ini (jika perlu) setelah meluncurkan bundel Grafik sehingga bundel lain menerima alamat IP yang diinginkan.

Secara default, pengaturan tetapkan alamat IPv6 secara otomatis dinonaktifkan. Untuk memeriksa pengaturan ini dari konsol Amazon VPC, pilih Subnet di panel navigasi. Pilih subnet, lalu pilih Tindakan, Ubah pengaturan penetapan IP otomatis.

Langkah 2: Tetapkan alamat IP publik ke alamat Anda WorkSpaces

Anda dapat menetapkan alamat IP publik ke alamat Anda WorkSpaces secara otomatis atau manual. Untuk menggunakan tugas otomatis, lihat the section called “Konfigurasikan alamat IP publik otomatis”. Untuk menetapkan alamat IP publik secara manual, gunakan prosedur berikut.

Untuk tutorial video tentang cara menetapkan alamat IP Elastis ke a WorkSpace, lihat video Pusat AWS Pengetahuan Bagaimana cara mengaitkan Alamat IP Elastis dengan? WorkSpace .

Untuk menetapkan alamat IP publik ke manual WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Perluas baris (pilih ikon panah) untuk WorkSpace dan perhatikan nilai WorkSpace IP. Ini adalah alamat IP pribadi utama dari WorkSpace.
4. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
5. Di panel navigasi, pilih IP Elastis. Jika Anda tidak memiliki alamat IP Elastis yang tersedia, pilih Mengaitkan alamat IP Elastis lalu pilih Grup alamat IPv4 Amazon atau Grup alamat IPv4 milik pelanggan, lalu pilih Alokasi. Catat alamat IP yang baru.
6. Di panel navigasi, pilih Antarmuka Jaringan.
7. Pilih antarmuka jaringan untuk Anda WorkSpace. Untuk menemukan antarmuka jaringan untuk Anda WorkSpace, masukkan nilai WorkSpace IP (yang Anda catat sebelumnya) di kotak pencarian, lalu tekan Enter. Nilai WorkSpace IP cocok dengan alamat IPv4 pribadi utama untuk antarmuka jaringan. Perhatikan bahwa ID VPC antarmuka jaringan cocok dengan ID WorkSpaces VPC Anda.
8. Pilih Tindakan, Kelola Alamat IP. Pilih Tetapkan IP baru, lalu pilih Ya, Perbarui. Catat alamat IP yang baru.
9. Pilih Tindakan, Kaitkan Alamat.
10. Pada halaman Kaitkan Alamat IP Elastis, pilih alamat IP Elastis dari Alamat. Untuk Kaitkan ke alamat IP privat, tentukan alamat IP privat baru, lalu pilih Kaitkan Alamat.

Zona Ketersediaan untuk Amazon WorkSpaces

Saat Anda membuat virtual private cloud (VPC) untuk digunakan dengan Amazon WorkSpaces, subnet VPC Anda harus berada di Availability Zone yang berbeda di Wilayah tempat Anda meluncurkan. WorkSpaces Availability Zone berada di lokasi yang berjauhan yang ditata sedemikian rupa agar terisolasi dari kegagalan Availability Zone lain. Dengan meluncurkan instans dalam Availability Zone yang terpisah, Anda dapat melindungi aplikasi Anda dari kegagalan di satu lokasi. Setiap subnet harus berada sepenuhnya dalam satu Availability Zone dan tidak dapat memperluas zona.

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

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

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

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

Nama Wilayah	Kode Wilayah	ID AZ yang didukung
US East (N. Virginia)	`us-east-1`	`use1-az2`, `use1-az4`, `use1-az6`
US West (Oregon)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`

Nama Wilayah	Kode Wilayah	ID AZ yang didukung
Asia Pasifik (Mumbai)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
Asia Pasifik (Seoul)	ap-northeast-2	apne2-az1 , apne2-az3
Asia Pasifik (Singapura)	ap-southeast-1	apse1-az1 , apse1-az2
Asia Pasifik (Sydney)	ap-southeast-2	apse2-az1 , apse2-az3
Asia Pasifik (Tokyo)	ap-northeast-1	apne1-az1 , apne1-az4
Kanada (Pusat)	ca-central-1	cac1-az1, cac1-az2
Eropa (Frankfurt)	eu-central-1	euc1-az2, euc1-az3
Eropa (Irlandia)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europe (London)	eu-west-2	euw2-az2, euw2-az3
Amerika Selatan (Sao Paulo)	sa-east-1	sae1-az1, sae1-az3
Afrika (Cape Town)	af-south-1	afs1-az1, afs1-az2, afs1-az3
Israel (Tel Aviv)	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3
AWS GovCloud (AS-Barat)	us-gov-west-1	usgw1-az1 , usgw1-az2 , usgw1-az3
AWS GovCloud (AS-Timur)	us-gov-east-1	usge1-az1 , usge1-az2 , usge1-az3

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

Alamat IP dan persyaratan port untuk WorkSpaces

Untuk terhubung ke Anda WorkSpaces, jaringan tempat WorkSpaces klien Anda terhubung harus memiliki port tertentu yang terbuka ke rentang alamat IP untuk berbagai AWS layanan (dikelompokkan dalam subset). Rentang alamat ini bervariasi menurut Wilayah AWS. Port yang sama juga harus terbuka pada firewall yang berjalan pada klien. Untuk informasi selengkapnya tentang rentang alamat AWS IP untuk Wilayah yang berbeda, lihat Rentang Alamat AWS IP di Referensi Umum Amazon Web Services.

Untuk diagram arsitektur, lihat WorkSpaces Arsitektur. Untuk diagram arsitektur tambahan, lihat Praktik Terbaik untuk Menerapkan Amazon. WorkSpaces

Port untuk aplikasi klien

Aplikasi WorkSpaces klien memerlukan akses keluar pada port berikut:

Port 53 (UDP)

Port ini digunakan untuk mengakses server DNS. Port harus terbuka untuk alamat IP server DNS Anda sehingga klien dapat menyelesaikan nama domain publik. Persyaratan port ini opsional jika Anda tidak menggunakan server DNS untuk resolusi nama domain.

Port 443 (TCP)

Port ini digunakan untuk pembaruan, pendaftaran, dan autentikasi aplikasi klien. Aplikasi klien desktop mendukung penggunaan server proksi untuk lalu lintas port 443 (HTTPS). Untuk memungkinkan penggunaan server proksi, buka aplikasi klien, pilih Pengaturan Lanjutan, pilih Gunakan Server Proxy, tentukan alamat dan port server proksi, dan pilih Simpan.

Port ini harus terbuka untuk rentang alamat IP berikut:

- Subset `AMAZON` di Wilayah `GLOBAL`.
- `AMAZON`Subset di Wilayah tempat WorkSpace berada.
- Subset `AMAZON` di Wilayah `us-east-1`.
- Subset `AMAZON` di Wilayah `us-west-2`.
- Subset `S3` di Wilayah `us-west-2`.

Port 4172 (UDP dan TCP)

Port ini digunakan untuk streaming WorkSpace desktop dan pemeriksaan kesehatan untuk PCoIP WorkSpaces. Port ini harus terbuka ke PCoIP Gateway dan ke server pemeriksaan kesehatan di

Wilayah tempat WorkSpace berada. Lihat informasi yang lebih lengkap di Server pemeriksaan kondisi dan Server gateway PCoIP.

Untuk PCoIP WorkSpaces, aplikasi klien desktop tidak mendukung penggunaan server proxy atau dekripsi TLS dan inspeksi untuk lalu lintas port 4172 di UDP (untuk lalu lintas desktop). Mereka membutuhkan koneksi langsung ke port 4172.

Port 4195 (UDP dan TCP)

Port ini digunakan untuk streaming WorkSpace desktop dan pemeriksaan kesehatan untuk WorkSpaces Streaming Protocol (WSP) WorkSpaces. Port ini harus terbuka untuk rentang alamat IP Gateway WSP dan server pemeriksaan kesehatan di Wilayah tempat WorkSpace berada. Lihat informasi yang lebih lengkap di Server pemeriksaan kondisi dan Server gateway WSP.

Untuk WSP WorkSpaces, aplikasi klien WorkSpaces Windows (versi 5.1 ke atas) dan aplikasi klien macOS (versi 5.4 ke atas) mendukung penggunaan server proxy HTTP untuk lalu lintas TCP port 4195, tetapi penggunaan proxy tidak disarankan. Dekripsi dan inspeksi TLS tidak didukung. Untuk informasi selengkapnya, lihat Mengkonfigurasi setelan server proxy perangkat untuk akses internet untuk Windows WorkSpaces, Amazon Linux WorkSpaces, dan Ubuntu WorkSpaces.

> **Note**
>
> - Jika firewall Anda menggunakan penyaringan stateful, port sementara (juga dikenal sebagai port dinamis) secara otomatis dibuka untuk memungkinkan komunikasi kembali. Jika firewall Anda menggunakan filter stateless, Anda harus membuka port sementara secara eksplisit untuk memungkinkan komunikasi kembali. Kisaran port sementara yang diperlukan yang harus Anda buka akan bervariasi tergantung pada konfigurasi Anda.
> - Fungsi server proxy tidak didukung untuk lalu lintas UDP. Jika Anda memilih untuk menggunakan server proxy, panggilan API yang dilakukan aplikasi klien ke WorkSpaces layanan Amazon juga diproksi. Panggilan API dan lalu lintas desktop harus melewati server proxy yang sama.

Port untuk Web Access

WorkSpaces Akses Web memerlukan akses keluar untuk port berikut:

Port 53 (UDP)

Port ini digunakan untuk mengakses server DNS. Port harus terbuka untuk alamat IP server DNS Anda sehingga klien dapat menyelesaikan nama domain publik. Persyaratan port ini opsional jika Anda tidak menggunakan server DNS untuk resolusi nama domain.

Port 80 (UDP dan TCP)

Port ini digunakan untuk hubungan awal ke `https://clients.amazonworkspaces.com`, yang kemudian beralih ke HTTPS. Itu harus terbuka untuk semua rentang alamat IP dalam `EC2` subset di Wilayah tempat WorkSpace berada.

Port 443 (UDP dan TCP)

Port ini digunakan untuk pendaftaran dan autentikasi menggunakan HTTPS. Itu harus terbuka untuk semua rentang alamat IP dalam `EC2` subset di Wilayah tempat WorkSpace berada.

Port 4195 (UDP dan TCP)

Untuk WorkSpaces yang dikonfigurasi untuk WorkSpaces Streaming Protocol (WSP), port ini digunakan untuk streaming lalu lintas WorkSpaces desktop. Port ini harus terbuka untuk rentang alamat IP Gateway WSP. Untuk informasi selengkapnya, lihat Server gateway WSP.

Akses web WSP mendukung penggunaan server proxy untuk port 4195 lalu lintas TCP, tetapi tidak disarankan. Untuk informasi selengkapnya, lihat Mengkonfigurasi setelan server proxy perangkat untuk akses internet untuk Windows WorkSpaces, Amazon Linux WorkSpaces, dan Ubuntu WorkSpaces.

> **Note**
>
> Jika firewall Anda menggunakan penyaringan stateful, port sementara (juga dikenal sebagai port dinamis) secara otomatis dibuka untuk memungkinkan komunikasi kembali. Jika firewall Anda menggunakan filter stateless, Anda harus membuka port sementara secara eksplisit untuk memungkinkan komunikasi kembali. Rentang port fana yang diperlukan yang harus Anda buka bervariasi tergantung pada konfigurasi Anda.

Biasanya, browser web secara acak memilih port sumber dalam kisaran tinggi untuk digunakan untuk streaming lalu lintas. WorkSpaces Akses Web tidak memiliki kontrol atas port yang dipilih browser. Anda harus memastikan bahwa lalu lintas kembali ke port ini diizinkan.

Domain dan alamat IP untuk ditambahkan ke daftar izin Anda

Agar aplikasi WorkSpaces klien dapat mengakses WorkSpaces layanan, Anda harus menambahkan domain dan alamat IP berikut ke daftar izinkan di jaringan tempat klien mencoba mengakses layanan.

Domain dan alamat IP untuk ditambahkan ke daftar izin Anda

Kategori	Domain atau Alamat IP
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	• https://d2td7dqidlhjx7.cloudfront.net/ • Di Wilayah AWS GovCloud (AS-Barat): https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/ WorkSpacesAppCastx 64.xml
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: • https://skylight-client-ds.us-east-1.amazonaws.com • https://skylight-client-ds.us-west-2.amazonaws.com • https://skylight-client-ds.ap-selatan-1.amazonaws.com • https://skylight-client-ds.ap-northeast-2.amazonaws.com • https://skylight-client-ds.ap-southeast-1.amazonaws.com • https://skylight-client-ds.ap-southeast-2.amazonaws.com • https://skylight-client-ds.ap-northeast-1.amazonaws.com • https://skylight-client-ds.ca-central-1.amazonaws.com

Kategori	Domain atau Alamat IP
	• https://skylight-client-ds.eu-central-1.amazonaws.com • https://skylight-client-ds.eu-west-1.amazonaws.com • https://skylight-client-ds.eu-west-2.amazonaws.com • https://skylight-client-ds.sa-east-1.amazonaws.com • https://skylight-client-ds.af-south-1.amazonaws.com • https://skylight-client-ds.il-central-1.amazonaws.com • Di Wilayah AWS GovCloud (AS-Barat): https://skylight-client-ds. us-gov-west-1.amazonaws.com • Di Wilayah AWS GovCloud (AS-Timur): https://skylight-client-ds. us-gov-east-1.amazonaws.com

Kategori	Domain atau Alamat IP
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.us-west-2.amazonaws.com • https://ws-client-service.ap-selatan-1.amazonaws.com • https://ws-client-service.ap-northeast-2.amazonaws.com • https://ws-client-service.ap-southeast-1.amazonaws.com • https://ws-client-service.ap-southeast-2.amazonaws.com • https://ws-client-service.ap-northeast-1.amazonaws.com • https://ws-client-service.ca-central-1.amazonaws.com • https://ws-client-service.eu-central-1.amazonaws.com • https://ws-client-service.eu-west-1.amazonaws.com • https://ws-client-service.eu-west-2.amazonaws.com • https://ws-client-service.sa-east-1.amazonaws.com • https://ws-client-service.af-south-1.amazonaws.com • https://ws-client-service.il-central-1.amazonaws.com • Di Wilayah AWS GovCloud (AS-Barat):

Kategori	Domain atau Alamat IP
	https://ws-client-service. us-gov-west-1.amazonaws.com • Di Wilayah AWS GovCloud (AS-Timur): https://ws-client-service. us-gov-east-1.amazonaws.com

Kategori	Domain atau Alamat IP
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • <region>Warisan - https://d1cbg795sa4g1u.cloudfront.net/prod//<directory ID> • AS Timur (Virginia N.) - https://d2h1yryv1jxiq.cloudfront.net/ • AS Barat (Oregon) - https://d1fq42e1gi7rtq.cloudfront.net/ • Asia Pasifik (Mumbai) - https://d1ctsk4u02kky7.cloudfront.net/ • Asia Pasifik (Seoul) - https://dyoj3cw6iktvg.cloudfront.net • Asia Pasifik (Singapura) - https://d1525ef92caquk.cloudfront.net/ • Asia Pasifik (Sydney) - https://dodwxjr2amr8p.cloudfront.net/

Kategori	Domain atau Alamat IP
	• Asia Pasifik (Tokyo) - https://d3v7kcib8ir2e1.cloudfront.net/ • Kanada (Tengah) - https://d1ebdk07rro1qy.cloudfront.net/ • Eropa (Frankfurt) - https://d39q4y7cndearu.cloudfront.net/ • Eropa (Irlandia) - https://d2127w6wvrc6l3.cloudfront.net/ • Eropa (London) - https://df4ahgpxbxqy2.cloudfront.net/ • Amerika Selatan (São Paulo) - https://d2nezqurrjvain.cloudfront.net/ • Afrika (Cape Town) - https://dr6ry0pwaoy23.cloudfront.net • Israel (Tel Aviv) - https://d2kmf63k5sit88.cloudfront.net File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • US East (N. Virginia) — https://d32i4gd7pg4909.cloudfront.net/ • US West (Oregon) — https://d18af777lco7lp.cloudfront.net/ • Asia Pacific (Mumbai) — https://d78hovzzqqtsb.cloudfront.net/ • Asia Pacific (Seoul) — https://dtyv4uwoh7ynt.cloudfront.net/

Kategori	Domain atau Alamat IP
	• Asia Pacific (Singapore) — https://d3qzmd7y07pz0i.cloudfront.net/ • Asia Pacific (Sydney) — https://dwcpoxuuza83q.cloudfront.net/ • Asia Pacific (Tokyo) — https://d2c2t8mxjhq5z1.cloudfront.net/ • Canada (Central) — https://d2wfbsypmqjmog.cloudfront.net/ • Europe (Frankfurt) — https://d1whcm49570jjw.cloudfront.net/ • Europe (Ireland) — https://d3pgffbf39h4k4.cloudfront.net/ • Europe (London) — https://d16q6638mh01s7.cloudfront.net/ • South America (São Paulo) — https://d2lh2qc5bdoq4b.cloudfront.net/ • Afrika (Cape Town) - https://di5ygl2cs0mrh.cloudfront.net/ • Israel (Tel Aviv) - https://d1a3pnge9on3sx.cloudfront.net Di Wilayah AWS GovCloud (AS-Barat): • Pengaturan direktori pelanggan: https://s3.amazonaws.com/ workspaces-client-properties /diprod/pdt/ <directory ID> • Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: https://workspace-client-assets-pdt.s3--1.amazonaws.com us-gov-west

Kategori	Domain atau Alamat IP
	• File CSS untuk memodifikasi halaman masuk: https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css • JavaScript berkas untuk halaman login: Tidak berlaku Di Wilayah AWS GovCloud (AS-Timur): • Pengaturan direktori pelanggan: https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID> • Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: https://workspace-client-assets-pdt.s3--1.amazonaws.com us-gov-east • File CSS untuk memodifikasi halaman masuk: https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css • JavaScript berkas untuk halaman login: Tidak berlaku
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi

Kategori	Domain atau Alamat IP
Titik Akhir Otentikasi Kartu Pintar Pra-sesi	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin. amazonaws-us-gov.com
Halaman Masuk Pengguna	https://<directory id>.awsapps.com/ (<directory id> adalah domain pelanggan) Di Wilayah AWS GovCloud (AS-Barat) dan AWS GovCloud (AS-Timur): https://login. us-gov-home<directory id><directory id>.awsapps.com/directory//(di mana domain pelanggan)

Kategori	Domain atau Alamat IP
Broker WS	Domain: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com • https://ws-broker-service.ap-selatan-1.amazonaws.com • https://ws-broker-service.ap-northeast-2.amazonaws.com • https://ws-broker-service.ap-southeast-1.amazonaws.com • https://ws-broker-service.ap-southeast-2.amazonaws.com • https://ws-broker-service.ap-northeast-1.amazonaws.com • https://ws-broker-service.ca-central-1.amazonaws.com • https://ws-broker-service.eu-central-1.amazonaws.com • https://ws-broker-service.eu-west-1.amazonaws.com • https://ws-broker-service.eu-west-2.amazonaws.com • https://ws-broker-service.sa-east-1.amazonaws.com • https://ws-broker-service.af-south-1.amazonaws.com

Kategori	Domain atau Alamat IP
	• https://ws-broker-service.il-central-1.amazonaws.com • https://ws-broker-service. us-gov-west-1.amazonaws.com • https://ws-broker-service-fips. us-gov-west-1.amazonaws.com • https://ws-broker-service. us-gov-east-1.amazonaws.com • https://ws-broker-service-fips. us-gov-east-1.amazonaws.com

Kategori	Domain atau Alamat IP
WorkSpaces Titik Akhir API	Domain: • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

Kategori	Domain atau Alamat IP
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces. us-gov-west-1.amazonaws.com • https://workspaces-fips. us-gov-west-1.amazonaws.com • https://workspaces. us-gov-east-1.amazonaws.com • https://workspaces-fips. us-gov-east-1.amazonaws.com

Kategori	Domain atau Alamat IP
WorkSpaces Titik Akhir untuk SALL Single Sign-On (SSO)	Domain: • https://euc-sso-sm.us-east-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.us-west-2.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.ap-south-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.eu-central-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.eu-west-2.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.af-south-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm.il-central-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm. us-gov-west-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm-fips. us-gov-west-1.amazonaws.com/v1/report-detak jantung

Kategori	Domain atau Alamat IP
	• https://euc-sso-sm. us-gov-east-1.amazonaws.com/v1/report-detak jantung • https://euc-sso-sm-fips. us-gov-east-1.amazonaws.com/v1/report-detak jantung

Domain dan alamat IP untuk ditambahkan ke daftar izin Anda untuk PCoIP

Kategori	Domain atau Alamat IP
Gateway Sesi PCoIP (PSG)	Server gateway PCoIP
Broker Sesi (PCM)	Domain: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com

Kategori	Domain atau Alamat IP
	• https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm. us-gov-west-1.amazonaws.com • https://skylight-cm-fips. us-gov-west-1.amazonaws.com • https://skylight-cm. us-gov-east-1.amazonaws.com • https://skylight-cm-fips. us-gov-east-1.amazonaws.com

Kategori	Domain atau Alamat IP
Server TURN Web Access untuk PCoIP	Server: • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • Web Access saat ini tidak tersedia di Wilayah Asia Pacific (Mumbai). • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • Akses Web saat ini tidak tersedia di Wilayah Afrika (Cape Town) • Akses Web saat ini tidak tersedia di Wilayah Israel (Tel Aviv).

Domain dan alamat IP untuk ditambahkan ke daftar izin Anda untuk Protokol WorkSpaces Streaming (WSP)

Kategori	Domain atau Alamat IP
Gateway Sesi WSP (WSG)	Server gateway WSP
Server TURN Web Access untuk WSP	Server gateway WSP

Server pemeriksaan kondisi

Aplikasi WorkSpaces klien melakukan pemeriksaan kesehatan melalui port 4172 dan 4195. Pemeriksaan ini memvalidasi apakah aliran lalu lintas TCP atau UDP dari WorkSpaces server ke aplikasi klien. Agar pemeriksaan ini berhasil selesai, kebijakan firewall Anda harus mengizinkan lalu lintas outbound ke alamat IP server pemeriksaan kondisi Wilayah berikut.

Wilayah	Hostname pemeriksaan kondisi	Alamat IP
US East (N. Virginia)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
US West (Oregon)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
Asia Pacific (Mumbai)	drp-bom.amazonworkspaces.com	13.127.57.82 13.234.250.73
Asia Pacific (Seoul)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105

Wilayah	Hostname pemeriksaan kondisi	Alamat IP
		52.78.44.253 52.79.54.102
Asia Pacific (Singapore)	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
Asia Pacific (Sydney)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
Asia Pacific (Tokyo)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
Canada (Central)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
Europe (Frankfurt)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227

Wilayah	Hostname pemeriksaan kondisi	Alamat IP
Europe (Ireland)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224
Europe (London)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
South America (São Paulo)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
Afrika (Cape Town)	drp-cpt.amazonworkspaces.com/	13.244.128.155 13.245.205.255 13.245.216.116
Israel (Tel Aviv)	drp-tlv.amazonworkspaces.com/	51.17.52.90 51.17.109.231 51.16.190.43

Wilayah	Hostname pemeriksaan kondisi	Alamat IP
AWS GovCloud (AS-Barat)	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88
AWS GovCloud (AS-Timur)	drp-osu.amazonworkspaces.com	18.253.251.70 18.254.0.118

Server gateway PCoIP

WorkSpaces menggunakan PCoIP untuk melakukan streaming sesi desktop ke klien melalui port 4172. Untuk server gateway PCoIP-nya, WorkSpaces menggunakan sejumlah kecil alamat IPv4 publik Amazon EC2. Ini memungkinkan Anda untuk mengatur kebijakan firewall yang lebih halus untuk perangkat yang mengakses WorkSpaces. Perhatikan bahwa WorkSpaces klien tidak mendukung alamat IPv6 sebagai opsi konektivitas saat ini.

Wilayah	Rentang alamat IP publik
US East (N. Virginia)	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
US West (Oregon)	35.80.88.0 - 35.80.95.255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255

Wilayah	Rentang alamat IP publik
Asia Pasifik (Mumbai)	13.126.243.0 - 13.126.243.255
Asia Pasifik (Seoul)	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
Asia Pasifik (Singapura)	18.141.152.0 - 18.141.152.255 18.141.154.0 - 18.141.155.255 52.76.127.0 - 52.76.127.255
Asia Pasifik (Sydney)	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
Asia Pasifik (Tokyo)	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
Kanada (Pusat)	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
Eropa (Frankfurt)	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255
Eropa (Irlandia)	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255

Wilayah	Rentang alamat IP publik
Eropa (London)	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
Amerika Selatan (Sao Paulo)	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255
Afrika (Cape Town)	13.246.120.0 - 13.246.123.255
Israel (Tel Aviv)	51.17.28.0-51.17.31.255
AWS GovCloud (AS-Barat)	52.61.193.0 - 52.61.193.255
AWS GovCloud (AS-Timur)	18.254.140.0 - 18.254.143.255

Server gateway WSP

> **Important**
>
> Mulai Juni 2020, WorkSpaces streaming sesi desktop untuk WSP WorkSpaces ke klien melalui port 4195, bukan port 4172. Jika Anda ingin menggunakan WSP WorkSpaces, pastikan port 4195 terbuka untuk lalu lintas.

WorkSpaces menggunakan sejumlah kecil alamat IPv4 publik Amazon EC2 untuk server gateway WSP-nya. Ini memungkinkan Anda untuk mengatur kebijakan firewall yang lebih halus untuk perangkat yang mengakses WorkSpaces. Perhatikan bahwa WorkSpaces klien tidak mendukung alamat IPv6 sebagai opsi konektivitas saat ini.

Wilayah	Rentang alamat IP publik
AS Timur (Virginia Utara)	• 3.227.4.0/22

Wilayah	Rentang alamat IP publik
	• 44.209.84.0/22
AS Barat (Oregon)	34.223.96.0/22
Asia Pasifik (Mumbai)	65.1.156.0/22
Asia Pasifik (Seoul)	3.35.160.0/22
Asia Pasifik (Singapura)	13.212.132.0/22
Asia Pasifik (Sydney)	3.25.248.0/22
Asia Pasifik (Tokyo)	3.114.164.0/22
Kanada (Pusat)	3.97.20.0/22
Eropa (Frankfurt)	18.192.216.0/22
Eropa (Irlandia)	3.248.176.0/22
Eropa (London)	18.134.68.0/22
Amerika Selatan (Sao Paulo)	15.228.64.0/22
Afrika (Cape Town)	13.246.108.0/22
Israel (Tel Aviv)	51.17.72.0/22
AWS GovCloud (AS-Barat)	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud (AS-Timur)	18.254.148.0/22

Nama domain gateway WSP

Tabel berikut mencantumkan nama domain WorkSpace gateway WSP. Domain-domain ini harus dapat dihubungi, agar aplikasi WorkSpaces klien dapat mengakses layanan WSP. WorkSpace

Wilayah	Domain
AS Timur (Virginia Utara)	*.prod.us-east-1.highlander.aws.a2z.com
AS Barat (Oregon)	*.prod.us-west-2.highlander.aws.a2z.com
Asia Pasifik (Mumbai)	*.prod.ap-selatan-1.highlander.aws.a2z.com
Asia Pasifik (Seoul)	*.prod.ap-northeast-2.highlander.aws.a2z.com
Asia Pasifik (Singapura)	*.prod.ap-southeast-1.highlander.aws.a2z.com
Asia Pasifik (Sydney)	*.prod.ap-southeast-2.highlander.aws.a2z.com
Asia Pasifik (Tokyo)	*.prod.ap-northeast-1.highlander.aws.a2z.com
Kanada (Pusat)	*.prod.ca-central-1.highlander.aws.a2z.com
Eropa (Frankfurt)	*.prod.eu-central-1.highlander.aws.a2z.com
Eropa (Irlandia)	*.prod.eu-west-1.highlander.aws.a2z.com
Eropa (London)	*.prod.eu-west-2.highlander.aws.a2z.com
Amerika Selatan (Sao Paulo)	*.prod.sa-east-1.highlander.aws.a2z.com
Afrika (Cape Town)	*.prod.af-selatan-1.highlander.aws.a2z.com
Israel (Tel Aviv)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud (AS-Barat)	*.prod. us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud (AS-Timur)	*.prod. us-gov-east-1.highlander.aws.a2z.com

Antarmuka jaringan

Masing-masing WorkSpace memiliki antarmuka jaringan berikut:

- Antarmuka jaringan utama (eth1) menyediakan konektivitas ke sumber daya dalam VPC Anda dan di internet, dan digunakan untuk bergabung WorkSpace ke direktori.

- Antarmuka jaringan manajemen (eth0) terhubung ke jaringan WorkSpaces manajemen yang aman. Ini digunakan untuk streaming interaktif WorkSpace desktop ke WorkSpaces klien, dan untuk memungkinkan WorkSpaces untuk mengelola WorkSpace.

WorkSpaces memilih alamat IP untuk antarmuka jaringan manajemen dari berbagai rentang alamat, tergantung pada Wilayah tempat WorkSpaces dibuat. Saat direktori terdaftar, WorkSpaces uji CIDR VPC dan tabel rute di VPC Anda untuk menentukan apakah rentang alamat ini menimbulkan konflik. Jika konflik ditemukan di semua rentang alamat yang tersedia di Wilayah, pesan kesalahan ditampilkan dan direktori tidak terdaftar. Jika Anda mengubah tabel rute di VPC Anda setelah direktori terdaftar, Anda mungkin menyebabkan konflik.

Warning

Jangan memodifikasi atau menghapus salah satu antarmuka jaringan yang dilampirkan ke file. WorkSpace Melakukan hal itu dapat WorkSpace menyebabkan menjadi tidak terjangkau atau kehilangan akses internet. Misalnya, jika Anda telah mengaktifkan penetapan otomatis alamat IP Elastis di tingkat direktori, alamat IP Elastis (dari kumpulan yang disediakan Amazon) ditetapkan ke alamat IP Anda WorkSpace saat diluncurkan. Namun, jika Anda mengaitkan alamat IP Elastis yang Anda miliki ke WorkSpace, dan kemudian Anda kemudian memisahkan alamat IP Elastis itu dari WorkSpace, alamat IP publiknya WorkSpace kehilangan, dan itu tidak secara otomatis mendapatkan yang baru dari kumpulan yang disediakan Amazon.
Untuk mengaitkan alamat IP publik baru dari kumpulan yang disediakan Amazon dengan WorkSpace, Anda harus membangun kembali. WorkSpace Jika Anda tidak ingin membangun kembali WorkSpace, Anda harus mengaitkan alamat IP Elastis lain yang Anda miliki ke alamat IP Elastic. WorkSpace

Rentang IP antarmuka manajemen

Tabel berikut mencantumkan rentang alamat IP yang digunakan untuk antarmuka jaringan manajemen.

Note

- Jika Anda menggunakan Windows Bring Your Own License (BYOL) WorkSpaces, rentang alamat IP dalam tabel berikut tidak berlaku. Sebagai gantinya, PCoIP BYOL WorkSpaces

menggunakan rentang alamat IP 54.239.224.0/20 untuk lalu lintas antarmuka manajemen di semua Wilayah. AWS Untuk WSP BYOL Windows WorkSpaces, rentang alamat IP 54.239.224.0/20 dan 10.0.0.0/8 berlaku di semua Wilayah. AWS (Rentang alamat IP ini digunakan selain blok/16 CIDR yang Anda pilih untuk lalu lintas manajemen untuk WorkSpaces BYOL Anda.)

- Jika Anda menggunakan WSP yang WorkSpaces dibuat dari bundel publik, rentang alamat IP 10.0.0.0/8 juga berlaku untuk lalu lintas antarmuka manajemen di semua AWS Wilayah, selain rentang PCOIP/WSP yang ditunjukkan pada tabel berikut.

Wilayah	Rentang alamat IP
AS Timur (Virginia Utara)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8
AS Barat (Oregon)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, dan 198.19.0.0/16 WSP: 10.0.0.0/8
Asia Pasifik (Mumbai)	PCoIP/WSP: 192.168.0.0/16 WSP: 10.0.0.0/8
Asia Pasifik (Seoul)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Asia Pasifik (Singapura)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Asia Pasifik (Sydney)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, dan 198.19.0.0/16 WSP: 10.0.0.0/8
Asia Pasifik (Tokyo)	PCoIP/WSP: 198.19.0.0/16

Wilayah	Rentang alamat IP
	WSP: 10.0.0.0/8
Kanada (Pusat)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Eropa (Frankfurt)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Eropa (Irlandia)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, dan 198.19.0.0/16 WSP: 10.0.0.0/8
Eropa (London)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Amerika Selatan (Sao Paulo)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Afrika (Cape Town)	PCOIP/WSP: 172.31.0.0/16 dan 198.19.0.0/16 WSP: 10.0.0.0/8
Israel (Tel Aviv)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
AWS GovCloud (AS-Barat)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8 dan 192.169.0.0/16
AWS GovCloud (AS-Timur)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

Port antarmuka manajemen

Port berikut harus terbuka pada antarmuka jaringan manajemen semua WorkSpaces:

- TCP inbound pada port 4172. Ini digunakan untuk pembentukan hubungan streaming pada protokol PCoIP.
- UDP inbound pada port 4172. Ini digunakan untuk streaming input pengguna pada protokol PCoIP.
- TCP inbound pada port 4489. Ini digunakan untuk akses menggunakan klien web.
- TCP inbound pada port 8200. Ini digunakan untuk manajemen dan konfigurasi WorkSpace.
- TCP inbound pada port 8201-8250. Port ini digunakan untuk pembentukan hubungan streaming dan untuk streaming input pengguna pada protokol WSP.
- UDP masuk di port 8220. Port ini digunakan untuk pembentukan koneksi streaming dan untuk streaming input pengguna pada protokol WSP
- TCP outbound pada port 8443 dan 9997. Ini digunakan untuk akses menggunakan klien web.
- UDP outbound pada port 3478, 4172, dan 4195. Ini digunakan untuk akses menggunakan klien web.
- UDP outbound pada port 50002 dan 55002. Ini digunakan untuk streaming. Jika firewall Anda menggunakan filter stateful, port sementara 50002 dan 55002 secara otomatis dibuka untuk memungkinkan komunikasi kembali. Jika firewall Anda menggunakan filter stateless, Anda harus membuka port sementara 49152 - 65535 untuk memungkinkan komunikasi kembali.
- TCP keluar pada port 80, seperti yang didefinisikan dalam rentang IP antarmuka Manajemen, ke alamat IP 169.254.169.254 untuk akses ke layanan metadata EC2. Proxy HTTP apa pun yang ditetapkan untuk Anda juga WorkSpaces harus mengecualikan 169.254.169.254.
- TCP outbound pada port 1688 ke alamat IP 169.254.169.250 dan 169.254.169.251 untuk mengizinkan akses ke Microsoft KMS untuk aktivasi Windows untuk Workspace yang didasarkan pada paket publik. Jika Anda menggunakan Windows Bring Your Own License (BYOL) WorkSpaces, Anda harus mengizinkan akses ke server KMS Anda sendiri untuk aktivasi Windows.
- Outbound TCP pada port 1688 ke alamat IP 54.239.236.220 untuk memungkinkan akses ke Microsoft KMS untuk aktivasi Office untuk BYOL. WorkSpaces

  Jika Anda menggunakan Office melalui salah satu bundel WorkSpaces publik, alamat IP untuk aktivasi Microsoft KMS untuk Office bervariasi. Untuk menentukan alamat IP itu, cari alamat IP untuk antarmuka manajemen WorkSpace, dan kemudian ganti dua oktet terakhir dengan. `64.250` Misalnya, jika alamat IP antarmuka manajemen 192.168.3.5, alamat IP untuk aktivasi Microsoft KMS Office adalah 192.168.64.250.

- Outbound TCP ke alamat IP 127.0.0.2 untuk WSP WorkSpaces ketika WorkSpace host dikonfigurasi untuk menggunakan server proxy.
- Komunikasi yang berasal dari alamat loopback 127.0.01.

Dalam keadaan normal, WorkSpaces layanan mengkonfigurasi port ini untuk Anda WorkSpaces. Jika ada perangkat lunak keamanan atau firewall yang diinstal pada port WorkSpace yang memblokir salah satu port ini, WorkSpace mungkin tidak berfungsi dengan benar atau mungkin tidak dapat dijangkau.

Port antarmuka utama

Apa pun jenis direktori yang Anda miliki, port berikut harus terbuka pada antarmuka jaringan utama semua WorkSpaces:

- Untuk konektivitas internet, port berikut harus terbuka keluar ke semua tujuan dan masuk dari WorkSpaces VPC. Anda perlu menambahkan ini secara manual ke grup keamanan untuk Anda WorkSpaces jika Anda ingin mereka memiliki akses internet.
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
- Untuk berkomunikasi dengan pengontrol direktori, port berikut harus terbuka antara WorkSpaces VPC Anda dan pengontrol direktori Anda. Untuk direktori Simple AD, grup keamanan yang dibuat oleh AWS Directory Service akan memiliki port ini yang dikonfigurasi dengan benar. Untuk direktori AD Connector, Anda mungkin perlu menyesuaikan grup keamanan default untuk VPC untuk membuka port ini.
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Autentikasi Kerberos
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP/UDP 636 - LDAP (LDAP melalui TLS/SSL)
  - TCP 1024-65535 - Port dinamis untuk RPC

Jika ada perangkat lunak keamanan atau firewall yang diinstal pada port WorkSpace yang memblokir salah satu port ini, WorkSpace mungkin tidak berfungsi dengan benar atau mungkin tidak dapat dijangkau.

Alamat IP dan persyaratan port menurut Wilayah

AS Timur (Virginia Utara)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.us-east-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.us-east-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan:

Kategori	Detail
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • US East (N. Virginia) — https://d32i4gd7pg4909.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Titik Akhir Otentikasi Kartu Pintar Pra-sesi	https://smartcard.us-east-1.signin.aws
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>

Kategori	Detail
Broker WS	Domain: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com
WorkSpaces Titik Akhir API	Domain: https://workspaces.us-east-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.us-east-1.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-iad.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
Server gateway PCoIP rentang alamat IP publik	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255

Kategori	Detail
Rentang alamat IP server gateway WSP	• 3.227.4.0/22 • 44.209.84.0/22
Nama domain gateway WSP	*.prod.us-east-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

AS Barat (Oregon)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.us-west-2.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.us-west-2.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID>

Kategori	Detail
	Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • US West (Oregon) — https://d18af777lco7lp.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Titik Akhir Otentikasi Kartu Pintar Pra-sesi	https://smartcard.us-west-2.signin.aws
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>

Kategori	Detail
Broker WS	Domain: • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.us-west-2.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-pdx.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140

Kategori	Detail
Server gateway PCoIP rentang alamat IP publik	• 35.80.88.0 - 35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
Rentang alamat IP server gateway WSP	34.223.96.0/22
Nama domain gateway WSP	*.prod.us-west-2.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia Pasifik (Mumbai)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.ap-selatan-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.ap-selatan-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace:

Kategori	Detail
	• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Asia Pacific (Mumbai) — https://d78hovzzqqtsb.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com

Kategori	Detail
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.ap-selatan-1.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.ap-south-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.ap-south-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Akses Web saat ini tidak tersedia di Wilayah Asia Pasifik (Mumbai)
Hostname pemeriksaan kondisi	drp-bom.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 13.127.57.82 • 13.234.250.73
Server gateway PCoIP rentang alamat IP publik	13.126.243.0 - 13.126.243.255
Rentang alamat IP server gateway WSP	65.1.156.0/22
Nama domain gateway WSP	*.prod.ap-selatan-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 192.168.0.0/16 • WSP: 10.0.0.0/8

Asia Pasifik (Seoul)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Perangkat (untuk 1.0+ dan 2.0+ aplikasi klien) WorkSpaces	https://-2.amazon.com/ device-metrics-us
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.ap-northeast-2.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.ap-northeast-2.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID>

Kategori	Detail
	Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Asia Pacific (Seoul) — https://dtyv4uwoh7ynt.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.ap-northeast-2.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.ap-northeast-2.amazonaws.com

Kategori	Detail
Broker Sesi (PCM)	Domain: • https://skylight-cm.ap-northeast-2.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.ap-northeast-2.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-icn.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
Server gateway PCoIP rentang alamat IP publik	• 3.34.37.0 - 3.34.37.255 • 3.34.38.0 - 3.34.39.255 • 13.124.247.0 - 13.124.247.255
Rentang alamat IP server gateway WSP	3.35.160.0/22
Nama domain gateway WSP	*.prod.ap-northeast-2.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia Pasifik (Singapura)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/

Kategori	Detail
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.ap-southeast-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.ap-southeast-1.amazonaws.com

Kategori	Detail
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Asia Pacific (Singapore) — https://d3qzmd7y07pz0i.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi

Kategori	Detail
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.ap-southeast-1.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.ap-southeast-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.ap-southeast-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.ap-southeast-1.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-sin.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
Server gateway PCoIP rentang alamat IP publik	• 18.141.152.0 - 18.141.152.255 • 18.141.154.0 - 18.141.155.255 • 52.76.127.0 - 52.76.127.255
Rentang alamat IP server gateway WSP	13.212.132.0/22

Kategori	Detail
Nama domain gateway WSP	*.prod.ap-southeast-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia Pasifik (Sydney)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.ap-southeast-2.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.ap-southeast-2.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/

Kategori	Detail
	Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Asia Pacific (Sydney) — https://dwcpoxuuza83q.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Titik Akhir Otentikasi Kartu Pintar Pra-sesi	https://smartcard.ap-southeast-2.signin.aws
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.ap-southeast-2.amazonaws.com

Kategori	Detail
WorkSpaces Titik Akhir API	Domain: • https://workspaces.ap-southeast-2.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.ap-southeast-2.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.ap-southeast-2.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-syd.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 3.24.11.127 • 13.237.232.125
Server gateway PCoIP rentang alamat IP publik	• 3.25.43.0 - 3.25.43.255 • 3.25.44.0 - 3.25.45.255 • 54.153.254.0 - 54.153.254.255
Rentang alamat IP server gateway WSP	3.25.248.0/22
Nama domain gateway WSP	*.prod.ap-southeast-2.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, dan 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia Pasifik (Tokyo)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.ap-northeast-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.ap-northeast-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding:

Kategori	Detail
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Asia Pacific (Tokyo) — https://d2c2t8mxjhq5z1.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Titik Akhir Otentikasi Kartu Pintar Pra-sesi	https://smartcard.ap-northeast-1.signin.aws
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.ap-northeast-1.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.ap-northeast-1.amazonaws.com

Kategori	Detail
Broker Sesi (PCM)	Domain: • https://skylight-cm.ap-northeast-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.ap-northeast-1.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-nrt.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 18.178.102.247 • 54.64.174.128
Server gateway PCoIP rentang alamat IP publik	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
Rentang alamat IP server gateway WSP	3.114.164.0/22
Nama domain gateway WSP	*.prod.ap-northeast-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Kanada (Pusat)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/

Kategori	Detail
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.ca-central-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.ca-central-1.amazonaws.com

Kategori	Detail
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Canada (Central) — https://d2wfbsypmqjmog.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi

Kategori	Detail
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.ca-central-1.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.ca-central-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.ca-central-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.ca-central-1.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-yul.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
Server gateway PCoIP rentang alamat IP publik	• 15.223.100.0 - 15.223.100.255 • 15.223.102.0 - 15.223.103.255 • 35.183.255.0 - 35.183.255.255
Rentang alamat IP server gateway WSP	3.97.20.0/22

Kategori	Detail
Nama domain gateway WSP	*.prod.ca-central-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Eropa (Frankfurt)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.eu-central-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.eu-central-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/

Kategori	Detail
	Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Europe (Frankfurt) — https://d1whcm49570jjw.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.eu-central-1.amazonaws.com

Kategori	Detail
WorkSpaces Titik Akhir API	Domain: • https://workspaces.eu-central-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.eu-central-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.eu-central-1.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-fra.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
Server gateway PCoIP rentang alamat IP publik	• 18.156.52.0 - 18.156.52.255 • 18.156.54.0 - 18.156.55.255 • 52.59.127.0 - 52.59.127.255
Rentang alamat IP server gateway WSP	18.192.216.0/22
Nama domain gateway WSP	*.prod.eu-central-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Eropa (Irlandia)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.eu-west-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.eu-west-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding:

Kategori	Detail
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Europe (Ireland) — https://d3pgffbf39h4k4.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Titik Akhir Otentikasi Kartu Pintar Pra-sesi	https://smartcard.eu-west-1.signin.aws
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.eu-west-1.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.eu-west-1.amazonaws.com

Kategori	Detail
Broker Sesi (PCM)	Domain: • https://skylight-cm.eu-west-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.eu-west-1.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-dub.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
Server gateway PCoIP rentang alamat IP publik	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255
Rentang alamat IP server gateway WSP	3.248.176.0/22
Nama domain gateway WSP	*.prod.eu-west-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, dan 198.19.0.0/16 • WSP: 10.0.0.0/8

Eropa (London)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/

Kategori	Detail
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.eu-west-2.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.eu-west-2.amazonaws.com

Kategori	Detail
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Europe (London) — https://d16q6638mh01s7.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi

Kategori	Detail
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.eu-west-2.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.eu-west-2.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.eu-west-2.amazonaws.com
Server TURN Web Access untuk PCoIP	Server: • turn:*.eu-west-2.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-lhr.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
Server gateway PCoIP rentang alamat IP publik	• 18.132.21.0 - 18.132.21.255 • 18.132.22.0 - 18.132.23.255 • 35.176.32.0 - 35.176.32.255
Rentang alamat IP server gateway WSP	18.134.68.0/22

Kategori	Detail
Nama domain gateway WSP	*.prod.eu-west-2.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Amerika Selatan (Sao Paulo)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.sa-east-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.sa-east-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/

Kategori	Detail
	Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • South America (São Paulo) — https://d2lh2qc5bdoq4b.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.sa-east-1.amazonaws.com

Kategori	Detail
WorkSpaces Titik Akhir API	Domain: • https://workspaces.sa-east-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.sa-east-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Peladen: • turn:*.sa-east-1.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-gru.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
Server gateway PCoIP rentang alamat IP publik	• 18.230.103.0 - 18.230.103.255 • 18.230.104.0 - 18.230.105.255 • 54.233.204.0 - 54.233.204.255
Rentang alamat IP server gateway WSP	15.228.64.0/22
Nama domain gateway WSP	*.prod.sa-east-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Afrika (Cape Town)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.af-south-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.af-south-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding:

Kategori	Detail
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Afrika (Cape Town); - https://di5ygl2cs0mrh.cloudfront.net/
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.af-south-1.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.af-south-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.af-south-1.amazonaws.com

Kategori	Detail
Hostname pemeriksaan kondisi	drp-cpt.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
Server gateway PCoIP rentang alamat IP publik	• 13.246.120.0 - 13.246.123.255
Rentang alamat IP server gateway WSP	15.228.64.0/22
Nama domain gateway WSP	*.prod.af-selatan-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• 172.31.0.0/16 dan 198.19.0.0/16 • WSP: 10.0.0.0/8

Israel (Tel Aviv)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://d2td7dqidlhjx7.cloudfront.net/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://skylight-client-ds.il-central-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service.il-central-1.amazonaws.com

Kategori	Detail
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • File CSS untuk memodifikasi halaman masuk: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript berkas untuk halaman login: • Israel (Tel Aviv); —
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com

Kategori	Detail
Halaman Masuk Pengguna	https://.awsapps.com/ (di mana domain pelanggan) <directory id><directory id>
Broker WS	Domain: • https://ws-broker-service.il-central-1.amazonaws.com
WorkSpaces Titik Akhir API	Domain: • https://workspaces.il-central-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm.il-central-1.amazonaws.com
Server TURN Web Access untuk PCoIP	Peladen: • giliran: *.il-central-1.rdn.amazonaws.com
Hostname pemeriksaan kondisi	drp-tlv.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
Server gateway PCoIP rentang alamat IP publik	• 51.17.28.0-51.17.31.255
Rentang alamat IP server gateway WSP	51.17.72.0/22
Nama domain gateway WSP	*.prod.il-central-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• 198.19.0.0/16 • WSP: 10.0.0.0/8

AWS GovCloud Wilayah (AS-Barat)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://s3.amazonaws.com/ workspaces-client-updates /dijual/pdt/windows/ WorkSpacesAppCast .xml/
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: hhttps://skylight-client-ds. us-gov-west-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service. us-gov-west-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://s3.amazonaws.com/ workspaces-client-properties /diprod/pdt/ <directory ID>

Kategori	Detail
	Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://s3.amazonaws.com/ workspaces-client-assets /diprod/pdt/ <directory ID> File CSS untuk memodifikasi halaman masuk: • https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css JavaScript berkas untuk halaman login: • Tidak berlaku
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Titik Akhir Otentikasi Kartu Pintar Pra-sesi	https://smartcard.signin. amazonaws-us-gov.com
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://login. us-gov-home<directory id><directory id>.awsapps.com/directory//(di mana domain pelanggan)
Broker WS	Domain: • https://ws-broker-service. us-gov-west-1.amazonaws.com • https://ws-broker-service-fips. us-gov-west-1.amazonaws.com

Kategori	Detail
WorkSpaces Titik Akhir API	Domain: • https://workspaces. us-gov-west-1.amazonaws.com • https://workspaces-fips. us-gov-west-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm. us-gov-west-1.amazonaws.com • https://skylight-cm-fips. us-gov-west-1.amazonaws.com
Hostname pemeriksaan kondisi	drp-pdt.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
Server gateway PCoIP rentang alamat IP publik	• 52.61.193.0 - 52.61.193.255
Rentang alamat IP server gateway WSP	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
Nama domain gateway WSP	*.prod. us-gov-west-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• 198.19.0.0/16 • WSP: 10.0.0.0/8 dan 192.169.0.0/16

AWS GovCloud Wilayah (AS-Timur)

Domain dan Alamat IP untuk ditambahkan ke daftar yang diizinkan

Kategori	Detail
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Pembaruan Otomatis Klien	https://s3.amazonaws.com/ workspaces-client-updates WorkSpacesAppCast /diprod/osu/ windows/ .xl
Pemeriksaan Konektivitas	https://connectivity.amazonworkspaces.com/
Metrik Klien (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: hhttps://skylight-client-ds. us-gov-east-1.amazonaws.com
Layanan Pesan Dinamis (untuk 3.0+ aplikasi WorkSpaces klien)	Domain: https://ws-client-service. us-gov-east-1.amazonaws.com
Pengaturan Direktori	Otentikasi dari klien ke direktori pelanggan sebelum login ke WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> Hubungan dari klien macOS: • https://d32i4gd7pg4909.cloudfront.net/ Pengaturan direktori pelanggan: • https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID>

Kategori	Detail
	Grafik halaman masuk untuk direktori pelanggan tingkat co-branding: • https://s3.amazonaws.com/ workspaces-client-assets /prod/osu/ <directory ID> File CSS untuk memodifikasi halaman masuk: • https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css JavaScript berkas untuk halaman login: • Tidak berlaku
Layanan Log Forrester	https://fls-na.amazon.com/
Server Pemeriksaan Kondisi (DRP)	Server pemeriksaan kondisi
Titik Akhir Otentikasi Kartu Pintar Pra-sesi	https://smartcard.signin. amazonaws-us-gov.com
Ketergantungan Pendaftaran (untuk Web Access dan Teradici Klien nol PCoIP)	https://s3.amazonaws.com
Halaman Masuk Pengguna	https://login. us-gov-home<directory id><directory id>.awsapps.com/directory//(di mana domain pelanggan)
Broker WS	Domain: • https://ws-broker-service. us-gov-east-1.amazonaws.com • https://ws-broker-service-fips. us-gov-east-1.amazonaws.com

Kategori	Detail
WorkSpaces Titik Akhir API	Domain: • https://workspaces. us-gov-east-1.amazonaws.com • https://workspaces-fips. us-gov-east-1.amazonaws.com
Broker Sesi (PCM)	Domain: • https://skylight-cm. us-gov-east-1.amazonaws.com • https://skylight-cm-fips. us-gov-east-1.amazonaws.com
Hostname pemeriksaan kondisi	drp-osu.amazonworkspaces.com
Alamat IP pemeriksaan kesehatan	• 18.253.251.70 • 18.254.0.118
Server gateway PCoIP rentang alamat IP publik	• 18.254.140.0 - 18.254.143.255
Rentang alamat IP server gateway WSP	18.254.148.0/22
Nama domain gateway WSP	*.prod. us-gov-east-1.highlander.aws.a2z.com
Antarmuka manajemen rentang alamat IP	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Persyaratan jaringan WorkSpaces klien Amazon

WorkSpaces Pengguna Anda dapat terhubung ke mereka WorkSpaces dengan menggunakan aplikasi klien untuk perangkat yang didukung. Atau, mereka dapat menggunakan browser web untuk terhubung ke WorkSpaces yang mendukung bentuk akses ini. Untuk daftar WorkSpaces yang mendukung akses browser web, lihat “ WorkSpaces Paket Amazon mana yang mendukung akses web?” di Akses client, Akses Web, dan Pengalaman Pengguna.

> **Note**
>
> Browser web tidak dapat digunakan untuk terhubung ke Amazon Linux WorkSpaces.

> **Important**
>
> Mulai 1 Oktober 2020, pelanggan tidak akan lagi dapat menggunakan klien Amazon WorkSpaces Web Access untuk terhubung ke kustom Windows 7 WorkSpaces atau ke Windows 7 Bring Your Own License (BYOL) WorkSpaces.

Untuk memberikan pengalaman yang baik kepada pengguna Anda WorkSpaces, verifikasi bahwa perangkat klien mereka memenuhi persyaratan jaringan berikut:

- Perangkat klien harus memiliki hubungan internet broadband. Kami merekomendasikan perencanaan untuk minimal 1 Mbps per pengguna simultan yang menonton jendela video 480p. Tergantung pada persyaratan kualitas pengguna untuk resolusi video, mungkin akan diperlukan bandwidth lebih besar.
- Jaringan tempat perangkat klien terhubung, dan firewall pada perangkat klien, harus memiliki port tertentu yang terbuka untuk rentang alamat IP untuk berbagai layanan AWS Untuk informasi selengkapnya, lihat Alamat IP dan persyaratan port untuk WorkSpaces.
- Untuk kinerja terbaik untuk PCoIP, waktu pulang pergi (RTT) dari jaringan klien ke Wilayah tempat tinggal harus kurang dari 100 ms. WorkSpaces Jika RTT antara 100ms dan 200ms, pengguna dapat mengakses WorkSpace, tetapi kinerja terpengaruh. Jika RTT antara 200ms dan 375ms, performanya menurun. Jika RTT melebihi 375ms, koneksi WorkSpaces klien dihentikan.

  Untuk kinerja terbaik untuk WorkSpaces Streaming Protocol (WSP), RTT dari jaringan klien ke Wilayah yang WorkSpaces berada di harus kurang dari 250ms. Jika RTT antara 250ms dan 400ms, pengguna dapat mengakses WorkSpace, tetapi kinerjanya menurun.

  Untuk memeriksa RTT ke berbagai AWS Wilayah dari lokasi Anda, gunakan Pemeriksaan Kesehatan WorkSpaces Koneksi Amazon.
- Untuk menggunakan webcam dengan WSP, kami merekomendasikan bandwidth unggahan dengan minimum 1,7 megabit per detik.
- Jika pengguna akan mengakses mereka WorkSpaces melalui jaringan pribadi virtual (VPN), koneksi harus mendukung unit transmisi maksimum (MTU) setidaknya 1200 byte.

> **Note**
>
> Anda tidak dapat mengakses WorkSpaces melalui VPN yang terhubung ke virtual private cloud (VPC) Anda. Untuk mengakses WorkSpaces menggunakan VPN, konektivitas internet (melalui alamat IP publik VPN) diperlukan, seperti yang dijelaskan dalamAlamat IP dan persyaratan port untuk WorkSpaces.

- Klien memerlukan akses HTTPS ke WorkSpaces sumber daya yang dihosting oleh layanan dan Amazon Simple Storage Service (Amazon S3). Klien tidak mendukung proksi pengalihan pada tingkat aplikasi. Akses HTTPS diperlukan agar pengguna dapat berhasil menyelesaikan pendaftaran dan mengaksesnya WorkSpaces.
- Untuk mengizinkan akses dari perangkat klien nol PCoIP, Anda harus menggunakan bundel protokol PCoIP untuk. WorkSpaces Anda juga harus mengaktifkan Network Time Protocol (NTP) di Teradici. Untuk informasi selengkapnya, lihat Siapkan klien nol PCoIP untuk WorkSpaces.
- Untuk 3.0+ klien, jika Anda menggunakan single sign-on (SSO) untuk Amazon WorkDocs, Anda harus mengikuti petunjuk di Single Sign-On di Panduan Administrasi. AWS Directory Service

Anda dapat memverifikasi bahwa perangkat klien memenuhi persyaratan jaringan sebagai berikut.

Untuk memverifikasi persyaratan jaringan untuk klien 3.0+

1. Buka WorkSpaces klien Anda. Jika ini adalah pertama kalinya Anda membuka klien, Anda akan diminta untuk memasukkan kode pendaftaran yang Anda terima dalam email undangan.
2. Tergantung pada klien yang Anda gunakan, lakukan salah satu hal berikut ini.

Jika Anda menggunakan...	Lakukan hal berikut
Klien Windows atau Linux	Di sudut kanan atas aplikasi klien, pilih ikon Jaringan .
Klien macOS	Pilih Hubungan, Jaringan.

   Aplikasi klien menguji hubungan jaringan, port, dan RTT, serta laporan hasil pengujian ini.
3. Tutup kotak dialog Jaringan untuk kembali ke halaman masuk.

Untuk memverifikasi persyaratan jaringan untuk klien 1.0+ dan 2.0+

1. Buka WorkSpaces klien Anda. Jika ini adalah pertama kalinya Anda membuka klien, Anda akan diminta untuk memasukkan kode pendaftaran yang Anda terima dalam email undangan.
2. Pilih Jaringan di sudut kanan bawah aplikasi klien. Aplikasi klien menguji hubungan jaringan, port, dan RTT, serta laporan hasil pengujian ini.
3. Pilih Abaikan untuk kembali ke halaman masuk.

Batasi WorkSpaces akses ke perangkat tepercaya

Secara default, pengguna dapat mengaksesnya WorkSpaces dari perangkat apa pun yang didukung yang terhubung ke internet. Jika perusahaan membatasi akses data perusahaan ke perangkat tepercaya (juga dikenal sebagai perangkat terkelola), Anda dapat membatasi WorkSpaces akses ke perangkat tepercaya dengan sertifikat yang valid.

Saat Anda mengaktifkan fitur ini, WorkSpaces gunakan otentikasi berbasis sertifikat untuk menentukan apakah perangkat dipercaya. Jika aplikasi WorkSpaces klien tidak dapat memverifikasi bahwa perangkat dipercaya, ia memblokir upaya untuk masuk atau menyambung kembali dari perangkat.

Untuk setiap direktori, Anda dapat mengimpor hingga dua sertifikat root. Jika Anda mengimpor dua root WorkSpaces certificate, berikan keduanya ke klien dan klien menemukan sertifikat pencocokan valid pertama yang menghubungkan ke salah satu root certificate.

Klien yang didukung

- Android, berjalan di Android atau sistem Chrome OS yang kompatibel dengan Android
- macOS
- Windows

> **Important**
>
> Fitur ini tidak didukung oleh klien berikut:
>
> - WorkSpaces aplikasi klien untuk Linux atau iPad

- Klien pihak ketiga, termasuk namun tidak terbatas pada, Teradici PCoIP, klien RDP, dan aplikasi desktop jarak jauh.

Langkah 1: Buat sertifikat

Fitur ini memerlukan dua tipe sertifikat: sertifikat root yang dihasilkan oleh Otoritas Sertifikasi (CA) internal dan sertifikat klien yang dirangkai hingga sertifikat root.

Persyaratan

- Sertifikat root harus berupa file sertifikat yang disandikan Base64 dalam format CRT, CERT, atau PEM.
- Sertifikat root harus memenuhi pola ekspresi reguler berikut, yang berarti bahwa setiap baris yang dikodekan, di samping yang terakhir, harus persis 64 karakter:. `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`
- Sertifikat perangkat harus menyertakan Nama Umum.
- Sertifikat perangkat harus menyertakan ekstensi berikut:`Key Usage: Digital Signature`, dan`Enhanced Key Usage: Client Authentication`.
- Semua sertifikat dalam rantai dari sertifikat perangkat ke Otoritas Sertifikat root tepercaya harus diinstal pada perangkat klien.
- Panjang maksimum rantai sertifikat yang didukung adalah 4.
- WorkSpaces Saat ini tidak mendukung mekanisme pencabutan perangkat, seperti daftar pencabutan sertifikat (CRL) atau Protokol Status Sertifikat Online (OCSP), untuk sertifikat klien.
- Gunakan algoritme enkripsi yang kuat. Kami merekomendasikan SHA256 dengan RSA, SHA256 dengan ECDSA, SHA384 dengan ECDSA, atau SHA512 dengan ECDSA.
- Untuk macOS, jika sertifikat perangkat ada di gantungan kunci sistem, kami sarankan Anda mengotorisasi aplikasi WorkSpaces klien untuk mengakses sertifikat tersebut. Jika tidak, pengguna harus memasukkan kredensial rantai kunci saat mereka masuk atau menghubungkan kembali.

Langkah 2: Deploy sertifikat klien ke perangkat tepercaya

Pada perangkat tepercaya untuk pengguna Anda, Anda harus menginstal bundel sertifikat yang mencakup semua sertifikat dalam rantai dari sertifikat perangkat ke Otoritas Sertifikat root tepercaya.

Anda dapat menggunakan solusi pilihan Anda untuk menginstal sertifikat ke armada perangkat klien Anda; misalnya, Manajer Konfigurasi Pusat Sistem (SCCM) atau manajemen perangkat seluler (MDM). Perhatikan bahwa SCCM dan MDM secara opsional dapat melakukan penilaian postur keamanan untuk menentukan apakah perangkat memenuhi kebijakan perusahaan Anda untuk mengakses. WorkSpaces

Aplikasi WorkSpaces klien mencari sertifikat sebagai berikut:

- Android - Buka Pengaturan, pilih Keamanan & lokasi, Kredensial, lalu pilih Instal dari kartu SD.
- Sistem Chrome OS yang kompatibel dengan Android - Buka pengaturan Android dan pilih Keamanan & lokasi, Kredensial, lalu pilih Instal dari kartu SD.
- macOS - Mencari rantai kunci untuk sertifikat klien.
- Windows - Mencari pengguna dan penyimpanan sertifikat root untuk sertifikat klien.

Langkah 3: Konfigurasikan batasan

Setelah Anda men-deploy sertifikat klien pada perangkat tepercaya, Anda dapat mengaktifkan akses terbatas di tingkat direktori. Ini mengharuskan aplikasi WorkSpaces klien untuk memvalidasi sertifikat pada perangkat sebelum mengizinkan pengguna untuk masuk ke file. WorkSpace

Untuk mengonfigurasi pembatasan

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori, lalu pilih Tindakan , Perbarui Detail.
4. Perluas Opsi Kontrol Akses .
5. Pilih jenis perangkat di bawah Untuk setiap jenis perangkat, tentukan perangkat mana yang dapat diakses WorkSpaces.
6. Impor hingga dua sertifikat root. Untuk setiap sertifikat root, lakukan hal berikut:
    a. Pilih Impor.
    b. Salin isi sertifikat ke formulir.
    c. Pilih Impor.
7. (Opsional) Tentukan apakah jenis perangkat lain memiliki akses ke WorkSpaces.

a. Gulir ke bawah ke bagian Platform Lain. Secara default, klien WorkSpaces Linux dinonaktifkan, dan pengguna dapat mengaksesnya WorkSpaces dari perangkat iOS, perangkat Android, Akses Web, Chromebook, dan perangkat klien nol PCoIP.

b. Pilih tipe perangkat untuk mengaktifkan dan menghapus tipe perangkat yang akan dinonaktifkan.

c. Untuk memblokir akses dari semua tipe perangkat yang dipilih, pilih Blok .

8. Pilih Perbarui dan Keluar.

WorkSpaces Integrasi dengan SAMP 2.0

Mengintegrasikan SAMP 2.0 dengan otentikasi sesi desktop Anda memungkinkan pengguna Anda WorkSpaces untuk menggunakan kredensi penyedia identitas SAMP 2.0 (iDP) yang ada dan metode otentikasi melalui browser web default mereka. Dengan menggunakan IDP Anda untuk mengautentikasi pengguna WorkSpaces, Anda dapat melindungi dengan WorkSpaces menggunakan fitur IDP seperti otentikasi multi-faktor dan kebijakan akses kontekstual.

Alur kerja autentikasi

Bagian berikut menjelaskan alur kerja otentikasi yang diprakarsai oleh aplikasi WorkSpaces klien, Akses WorkSpaces Web, dan penyedia identitas SAMP 2.0 (iDP):

- Ketika aliran diprakarsai oleh iDP. Misalnya, ketika pengguna memilih aplikasi di portal pengguna IDP di browser web.
- Ketika aliran diprakarsai oleh WorkSpaces klien. Misalnya, ketika pengguna membuka aplikasi klien dan masuk.
- Ketika aliran diprakarsai oleh akses WorkSpaces Web. Misalnya, ketika pengguna membuka Akses Web di browser dan masuk.

Dalam contoh ini, pengguna masuk `user@example.com` untuk masuk ke iDP. IDP memiliki aplikasi penyedia layanan SAMP 2.0 yang dikonfigurasi untuk WorkSpaces direktori dan pengguna diberi wewenang untuk aplikasi WorkSpaces SAMP 2.0. Pengguna membuat WorkSpace untuk nama pengguna mereka,`user`, di direktori yang diaktifkan untuk otentikasi SAMP 2.0. Selain itu, pengguna menginstal aplikasi WorkSpaces klien di perangkat mereka atau pengguna menggunakan Akses Web di browser web.

Aliran yang dimulai oleh penyedia identitas (iDP) dengan aplikasi klien

Alur yang diprakarsai IDP memungkinkan pengguna untuk secara otomatis mendaftarkan aplikasi WorkSpaces klien di perangkat mereka tanpa harus memasukkan kode registrasi. WorkSpaces Pengguna tidak masuk WorkSpaces menggunakan alur yang diprakarsai IDP. WorkSpaces otentikasi harus berasal dari aplikasi klien.

1. Menggunakan browser web mereka, pengguna masuk ke iDP.
2. Setelah masuk ke iDP, pengguna memilih WorkSpaces aplikasi dari portal pengguna iDP.
3. Pengguna diarahkan ke halaman ini di browser, dan aplikasi WorkSpaces klien dibuka secara otomatis.

4. Aplikasi WorkSpaces klien sekarang terdaftar dan pengguna dapat terus masuk dengan mengklik Lanjutkan untuk masuk WorkSpaces.

Aliran yang dimulai oleh penyedia identitas (iDP) dengan Akses Web

Aliran Akses Web yang diprakarsai IDP memungkinkan pengguna untuk secara otomatis mendaftarkan mereka WorkSpaces melalui browser web tanpa harus memasukkan kode registrasi. WorkSpaces Pengguna tidak masuk WorkSpaces menggunakan alur yang diprakarsai IDP. WorkSpaces otentikasi harus berasal dari Web Access.

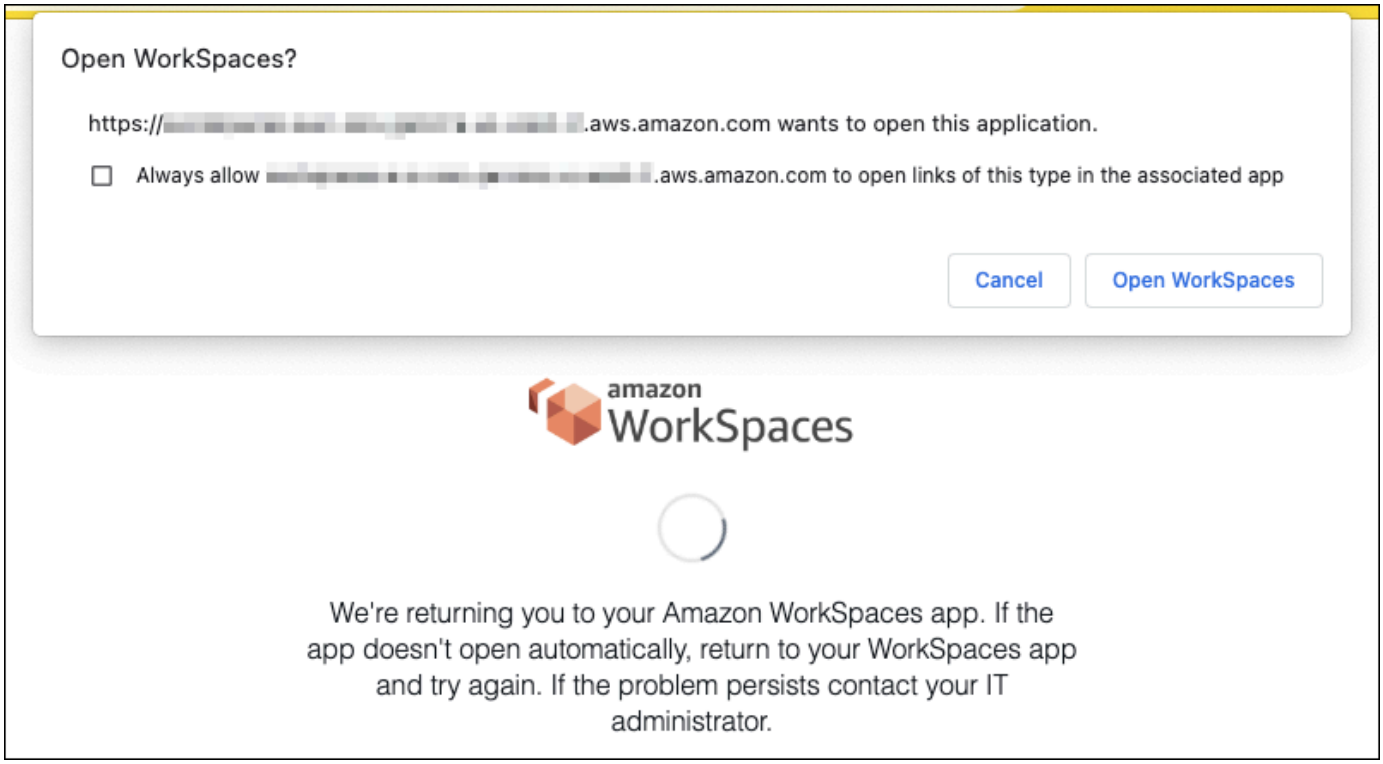
1. Menggunakan browser web mereka, pengguna masuk ke iDP.
2. Setelah masuk ke iDP, pengguna mengklik WorkSpaces aplikasi dari portal pengguna iDP.
3. Pengguna diarahkan ke halaman ini di browser. Untuk membuka WorkSpaces, pilih Amazon WorkSpaces di browser.

4. Aplikasi WorkSpaces klien sekarang terdaftar dan pengguna dapat terus masuk melalui Akses WorkSpaces Web.

WorkSpaces aliran yang diprakarsai klien

Alur yang diprakarsai klien memungkinkan pengguna untuk masuk ke akun mereka WorkSpaces setelah masuk ke iDP.

1. Pengguna meluncurkan aplikasi WorkSpaces klien (jika belum berjalan) dan mengklik Lanjutkan untuk WorkSpaces masuk.
2. Pengguna diarahkan ke browser web default mereka untuk masuk ke iDP. Jika pengguna sudah masuk ke iDP di browser mereka, mereka tidak perlu masuk lagi dan akan melewati langkah ini.
3. Setelah masuk ke iDP, pengguna akan diarahkan ke pop up. Ikuti petunjuk untuk memungkinkan browser web Anda membuka aplikasi klien.



4. Pengguna diarahkan ke aplikasi WorkSpaces klien untuk menyelesaikan masuk ke aplikasi mereka WorkSpace. WorkSpaces nama pengguna diisi secara otomatis dari pernyataan IDP SAMP 2.0. Saat Anda menggunakan otentikasi berbasis sertifikat (CBA), pengguna secara otomatis masuk.
5. Pengguna masuk ke mereka WorkSpace.

WorkSpaces Alur yang diprakarsai oleh Akses Web

Alur yang diprakarsai Akses Web memungkinkan pengguna untuk masuk ke akun mereka WorkSpaces setelah masuk ke iDP.

1. Pengguna meluncurkan Akses WorkSpaces Web dan memilih Masuk.
2. Di tab browser yang sama, pengguna diarahkan ke portal iDP. Jika pengguna sudah masuk ke iDP di browser mereka, mereka tidak perlu masuk lagi dan dapat melewati langkah ini.
3. Setelah masuk ke iDP, pengguna diarahkan ke halaman ini di browser, dan klik Masuk ke. WorkSpaces
4. Pengguna dialihkan ke aplikasi WorkSpaces klien untuk menyelesaikan masuk ke aplikasi mereka WorkSpace. WorkSpaces nama pengguna diisi secara otomatis dari pernyataan IDP SAMP 2.0. Saat Anda menggunakan otentikasi berbasis sertifikat (CBA), pengguna secara otomatis masuk.

5. Pengguna masuk ke mereka WorkSpace.

Menyiapkan SAMP 2.0

Aktifkan pendaftaran aplikasi WorkSpaces klien dan masuk WorkSpaces untuk pengguna Anda dengan menggunakan kredensi dan metode otentikasi penyedia identitas SAMP 2.0 (IDP) mereka dengan menyiapkan federasi identitas menggunakan SAMP 2.0. Untuk mengatur federasi identitas menggunakan SAMP 2.0, gunakan peran IAM dan URL status relai untuk mengonfigurasi IDP Anda dan mengaktifkan. AWS Ini memberi pengguna federasi Anda akses ke direktori. WorkSpaces Status relai adalah titik akhir WorkSpaces direktori tempat pengguna diteruskan setelah berhasil masuk. AWS

Daftar Isi

Persyaratan

- Otentikasi SAMP 2.0 tersedia di Wilayah berikut:
  - Wilayah AS Timur (Virginia Utara)
  - Wilayah AS Barat (Oregon)
  - Wilayah Afrika (Cape Town)
  - Wilayah Asia Pacific (Mumbai)
  - Wilayah Asia Pasifik (Seoul)
  - Wilayah Asia Pasifik (Singapura)
  - Wilayah Asia Pasifik (Sydney)

  - Wilayah Asia Pasifik (Tokyo)
  - Wilayah Kanada (Pusat)
  - Wilayah Eropa (Frankfurt)
  - Wilayah Eropa (Irlandia)
  - Wilayah Eropa (London)
  - Wilayah Amerika Selatan (Sao Paulo)
  - Wilayah Israel (Tel Aviv)
  - AWS GovCloud (AS-Barat)
  - AWS GovCloud (AS-Timur)
- Untuk menggunakan otentikasi SAMP 2.0 WorkSpaces, IDP harus mendukung SSO yang diprakarsai IDP yang tidak diminta dengan sumber daya target deep link atau URL titik akhir status relai. Contohnya IdPs termasuk ADFS, Azure AD, Duo Single Sign-On, Okta, dan. PingFederate PingOne Konsultasikan dokumentasi IDP Anda untuk informasi lebih lanjut.
- Otentikasi SAMP 2.0 akan berfungsi dengan WorkSpaces diluncurkan menggunakan Simple AD, tetapi ini tidak disarankan karena Simple AD tidak terintegrasi dengan SAMP 2.0. IdPs
- Otentikasi SAMP 2.0 didukung pada klien berikut WorkSpaces . Versi klien lainnya tidak didukung untuk otentikasi SAMP 2.0. Buka Unduhan WorkSpaces Klien Amazon untuk menemukan versi terbaru:
  - Aplikasi klien Windows versi 5.1.0.3029 atau yang lebih baru
  - klien macOS versi 5.x atau yang lebih baru
  - Akses Web

  Versi klien lain tidak akan dapat terhubung ke WorkSpaces diaktifkan untuk otentikasi SAMP 2.0 kecuali fallback diaktifkan. Untuk informasi selengkapnya, lihat Mengaktifkan otentikasi SAMP 2.0 di direktori. WorkSpaces

Untuk step-by-step petunjuk mengintegrasikan SAMP 2.0 dengan WorkSpaces menggunakan ADFS, Azure AD, Duo Single Sign-On, Okta, dan PingFederate untuk PingOne Enterprise, tinjau Panduan OneLogin Implementasi Otentikasi Amazon SAMP. WorkSpaces

Prasyarat

Selesaikan prasyarat berikut sebelum mengonfigurasi koneksi penyedia identitas SAMP 2.0 (iDP) Anda ke direktori. WorkSpaces

1. Konfigurasikan IDP Anda untuk mengintegrasikan identitas pengguna dari Microsoft Active Directory yang digunakan dengan direktori. WorkSpaces Untuk pengguna dengan WorkSpace atribut sAM AccountName dan email untuk pengguna Active Directory dan nilai klaim SAMP harus cocok dengan pengguna untuk masuk WorkSpaces menggunakan iDP. Untuk informasi selengkapnya tentang mengintegrasikan Active Directory dengan IDP Anda, lihat dokumentasi IDP Anda.
2. Konfigurasikan IdP Anda untuk membuat hubungan kepercayaan dengan AWS.
   - Lihat Mengintegrasikan penyedia solusi SAMP pihak ketiga dengan AWS untuk informasi selengkapnya tentang mengonfigurasi AWS federasi. Contoh yang relevan termasuk integrasi iDP dengan AWS IAM untuk mengakses konsol manajemen. AWS
   - Gunakan iDP Anda untuk membuat dan mengunduh dokumen metadata federasi yang menjelaskan organisasi Anda sebagai IDP. Dokumen XHTML yang ditandatangani ini digunakan untuk membangun kepercayaan pihak yang mengandalkan. Simpan file ini ke lokasi yang dapat Anda akses dari konsol IAM nanti.
3. Buat atau daftarkan direktori WorkSpaces dengan menggunakan konsol WorkSpaces manajemen. Untuk informasi selengkapnya, lihat Mengelola direktori untuk WorkSpaces. Otentikasi SAMP 2.0 untuk WorkSpaces didukung untuk jenis direktori berikut:
   - AD Connector
   - Microsoft AD yang Dikelola AWS
4. Buat WorkSpace untuk pengguna yang dapat masuk ke iDP menggunakan jenis direktori yang didukung. Anda dapat membuat WorkSpace menggunakan konsol WorkSpaces manajemen,AWS CLI, atau WorkSpaces API. Untuk informasi selengkapnya, lihat Meluncurkan desktop virtual menggunakan WorkSpaces.

Langkah 1: Buat penyedia identitas SAMP di AWS IAM

Pertama, buat SAMP iDP AWS di IAM. IDP ini mendefinisikan hubungan AWS IDP-to-trust organisasi Anda menggunakan dokumen metadata yang dihasilkan oleh perangkat lunak iDP di organisasi Anda. Untuk informasi selengkapnya, lihat Membuat dan mengelola penyedia identitas SAMP (Amazon Web Services Management Console). Untuk informasi tentang bekerja dengan SAMP IdPs di AWS GovCloud (AS-Barat) dan AWS GovCloud (AS-Timur), lihat AWSIdentity and Access Management.

Langkah 2: Buat peran IAM federasi SAMP 2.0

Selanjutnya, buat peran IAM federasi SAMP 2.0. Langkah ini menetapkan hubungan kepercayaan antara IAM dan IDP organisasi Anda, yang mengidentifikasi IDP Anda sebagai entitas tepercaya untuk federasi.

Untuk membuat peran IAM untuk SAMP iDP

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran > Buat peran.
3. Untuk tipe Peran, pilih federasi SAMP 2.0.
4. Untuk SAMP Provider pilih IDP SALL yang Anda buat.

> **Important**
>
> Jangan memilih salah satu dari dua metode akses SAMP 2.0, Izinkan akses terprogram saja atau Izinkan akses Konsol Manajemen Layanan Amazon Web Services dan terprogram.

5. Untuk Atribut, pilih SAML:SUB_TYPE.
6. Untuk Nilai masukkan`persistent`. Nilai ini membatasi akses peran ke permintaan streaming pengguna SAMP yang menyertakan pernyataan tipe subjek SAMP dengan nilai persisten. Jika SAML:sub_type persisten, IDP Anda mengirimkan nilai unik yang sama untuk elemen NameID di semua permintaan SAMP dari pengguna tertentu. Untuk informasi selengkapnya tentang pernyataan SAML:sub_type, lihat bagian Mengidentifikasi pengguna secara unik di federasi berbasis SAMP di Menggunakan federasi berbasis SAMP untuk akses API. AWS
7. Tinjau informasi kepercayaan SAMP 2.0 Anda, konfirmasikan entitas dan kondisi tepercaya yang benar, lalu pilih Berikutnya: Izin.
8. Pada halaman Lampirkan kebijakan izin, pilih Berikutnya: Tag.
9. (Opsional) Masukkan kunci dan nilai untuk setiap tag yang ingin Anda tambahkan. Untuk informasi selengkapnya, lihat Menandai pengguna dan peran IAM.
10. Setelah selesai, pilih Berikutnya: Tinjau. Anda akan membuat dan menyematkan kebijakan inline untuk peran ini nanti.
11. Untuk nama Peran, masukkan nama yang mengidentifikasi tujuan peran ini. Karena beberapa entitas mungkin mereferensikan peran, Anda tidak dapat mengedit nama peran setelah dibuat.

12. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
13. Tinjau detail peran dan pilih Buat peran.
14. Tambahkan TagSession izin sts: ke kebijakan kepercayaan peran IAM baru Anda. Untuk informasi selengkapnya, lihat Melewati tag sesi di AWS STS. Di detail peran IAM baru Anda, pilih tab Trust relationship, lalu pilih Edit trust relationship*. Saat editor kebijakan Edit Trust Relationship terbuka, tambahkan izin sts: TagSession *, sebagai berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:sub_type": "persistent"
        }
      }
    }
  ]
}
```

Ganti `IDENTITY-PROVIDER` dengan nama SAMP iDP yang Anda buat di Langkah 1. Kemudian pilih Perbarui Kebijakan Kepercayaan.

Langkah 3: Sematkan kebijakan inline untuk peran IAM

Selanjutnya, sematkan kebijakan IAM sebaris untuk peran yang Anda buat. Saat Anda menyematkan kebijakan sebaris, izin dalam kebijakan tersebut tidak dapat secara tidak sengaja dilampirkan ke entitas utama yang salah. Kebijakan inline memberi pengguna federasi akses ke direktori. WorkSpaces

> **Important**
>
> Kebijakan IAM untuk mengelola akses AWS berdasarkan IP sumber tidak didukung untuk `workspaces:Stream` tindakan tersebut. Untuk mengelola kontrol akses IP WorkSpaces, gunakan grup kontrol akses IP. Selain itu, saat menggunakan otentikasi SAMP 2.0, Anda dapat menggunakan kebijakan kontrol akses IP jika tersedia dari SAMP 2.0 IDP Anda.

1. Dalam detail untuk peran IAM yang Anda buat, pilih tab Izin, lalu tambahkan izin yang diperlukan ke kebijakan izin peran. Wizard Create policy akan dimulai.
2. Di Buat kebijakan, pilih tab JSON.
3. Salin dan tempel kebijakan JSON berikut ke jendela JSON. Kemudian, ubah sumber daya dengan memasukkan Kode AWS Wilayah, ID akun, dan ID direktori Anda. Dalam kebijakan berikut, `"Action": "workspaces:Stream"` adalah tindakan yang memberi WorkSpaces pengguna Anda izin untuk terhubung ke sesi desktop mereka di WorkSpaces direktori.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

Ganti `REGION-CODE` dengan AWS Wilayah tempat WorkSpaces direktori Anda ada. Ganti `DIRECTORY-ID` dengan ID WorkSpaces direktori, yang dapat ditemukan di konsol WorkSpaces manajemen. Untuk sumber daya di AWS GovCloud (AS-Barat) atau AWS GovCloud (AS-

Timur), gunakan format berikut untuk ARN:. `arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`

4. Setelah selesai, pilih Kebijakan tinjau. Validator Kebijakan akan melaporkan kesalahan sintaks apa pun.

Langkah 4: Konfigurasikan penyedia identitas SAMP 2.0 Anda

Selanjutnya, tergantung pada IDP SAMP 2.0 Anda, Anda mungkin perlu memperbarui IDP Anda secara manual agar AWS dipercaya sebagai penyedia layanan dengan mengunggah `saml-metadata.xml` file di https://signin.aws.amazon.com/static/saml-metadata.xml ke IDP Anda. Langkah ini memperbarui metadata IDP Anda. Bagi sebagian orang IdPs, pembaruan mungkin sudah dikonfigurasi. Jika ini masalahnya, lanjutkan ke langkah berikutnya.

Jika pembaruan ini belum dikonfigurasi di IDP Anda, tinjau dokumentasi yang disediakan oleh iDP Anda untuk informasi tentang cara memperbarui metadata. Beberapa penyedia memberi Anda opsi untuk mengetik URL, dan iDP memperoleh dan menginstal file untuk Anda. Lainnya mengharuskan Anda mengunduh file dari URL lalu menyediakannya sebagai file lokal.

> **Important**
>
> Pada saat ini, Anda juga dapat memberi wewenang kepada pengguna di IDP Anda untuk mengakses aplikasi yang telah Anda konfigurasikan WorkSpaces di iDP Anda. Pengguna yang berwenang untuk mengakses WorkSpaces aplikasi untuk direktori Anda tidak secara otomatis memiliki yang WorkSpace dibuat untuk mereka. Demikian juga, pengguna yang telah WorkSpace dibuat untuk mereka tidak secara otomatis diizinkan untuk mengakses WorkSpaces aplikasi. Agar berhasil terhubung ke otentikasi WorkSpace menggunakan SAMP 2.0, pengguna harus diberi wewenang oleh iDP dan harus memiliki yang dibuat. WorkSpace

Langkah 5: Buat pernyataan untuk respons otentikasi SAMP

Selanjutnya, konfigurasikan informasi yang dikirim IDP Anda AWS sebagai atribut SAMP dalam respons otentikasi. Bergantung pada IDP Anda, ini sudah dikonfigurasi, lewati langkah ini dan lanjutkan ke Langkah 6: Konfigurasikan status relai federasi Anda.

Jika informasi ini belum dikonfigurasi di IDP Anda, berikan yang berikut ini:

- NameID Subjek SAMP — Pengidentifikasi unik untuk pengguna yang masuk. Nilai harus cocok dengan nama WorkSpaces pengguna, dan biasanya AccountName atribut SAM untuk pengguna Active Directory.
- Jenis Subjek SAMP (dengan nilai yang disetel ke`persistent`) - Mengatur nilai untuk `persistent` memastikan bahwa IDP Anda mengirimkan nilai unik yang sama untuk elemen `NameID` di semua permintaan SAMP dari pengguna tertentu. Pastikan bahwa kebijakan IAM Anda menyertakan kondisi untuk hanya mengizinkan permintaan SAMP dengan sub_type SAMP yang disetel ke`persistent`, seperti yang dijelaskan pada Langkah 2: Buat peran IAM federasi SAMP 2.0.
- **`Attribute`**elemen dengan **`Name`** atribut disetel ke **`https://aws.amazon.com/SAML/Attributes/Role`** - Elemen ini berisi satu atau lebih `AttributeValue` elemen yang mencantumkan peran IAM dan SAMP iDP yang pengguna dipetakan oleh idP Anda. Peran dan idP ditentukan sebagai pasangan ARN yang dibatasi koma. Contoh dari nilai yang diharapkan adalah`arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`.
- **`Attribute`**elemen dengan **`Name`** atribut disetel ke **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** - Elemen ini berisi satu `AttributeValue` elemen yang menyediakan pengenal untuk kredensi AWS sementara yang dikeluarkan untuk SSO. Nilai dalam **`AttributeValue`** elemen harus antara 2 dan 64 karakter, hanya dapat berisi karakter alfanumerik, garis bawah, dan karakter berikut: _. :/= + - @. Itu tidak bisa berisi spasi. Nilai biasanya alamat email atau nama utama pengguna (UPN). Seharusnya bukan nilai yang menyertakan spasi, seperti nama tampilan pengguna.
- **`Attribute`**elemen dengan **`Name`** atribut diatur ke **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** - Elemen ini berisi satu `AttributeValue` elemen yang menyediakan alamat email pengguna. Nilai harus sesuai dengan alamat email WorkSpaces pengguna seperti yang didefinisikan dalam WorkSpaces direktori. Nilai tag dapat mencakup kombinasi huruf, angka, spasi, dan _.:/= + - @ karakter. Untuk informasi selengkapnya, lihat Aturan untuk menandai di IAM dan AWS STS di Panduan Pengguna IAM.
- **`Attribute`**elemen dengan **`Name`** atribut diatur ke **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** (opsional) - Elemen ini berisi satu `AttributeValue` elemen yang menyediakan Direktori Aktif `userPrincipalName` untuk pengguna yang masuk. Nilai harus disediakan dalam format`username@domain.com`. Parameter ini digunakan dengan otentikasi berbasis sertifikat sebagai Nama Alternatif Subjek di sertifikat pengguna akhir. Untuk informasi selengkapnya, lihat Otentikasi Berbasis Sertifikat.

- **`Attribute`**elemen dengan **`Name`** atribut diatur ke **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`** (opsional) - Elemen ini berisi satu `AttributeValue` elemen yang menyediakan pengenal keamanan Direktori Aktif (SID) untuk pengguna yang masuk. Parameter ini digunakan dengan otentikasi berbasis sertifikat untuk mengaktifkan pemetaan yang kuat ke pengguna Active Directory. Untuk informasi selengkapnya, lihat Otentikasi Berbasis Sertifikat.
- **`Attribute`**elemen dengan **`Name`** atribut diatur ke **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName`** (opsional) - Elemen ini berisi satu `AttributeValue` elemen yang menyediakan format nama pengguna alternatif. Gunakan atribut ini jika Anda memiliki kasus penggunaan yang memerlukan format nama pengguna seperti`corp\username`,`corp.example.com\username`, atau `username@corp.example.com` untuk masuk menggunakan WorkSpaces klien. Kunci dan nilai tag dapat mencakup kombinasi huruf, angka, spasi, dan _:/. + = @ - karakter. Untuk informasi selengkapnya, lihat Aturan untuk menandai di IAM dan AWS STS di Panduan Pengguna IAM. Untuk mengklaim `corp\username` atau `corp.example.com\username` format, ganti\ dengan/dalam pernyataan SAMP.
- **`Attribute`**elemen dengan **`Name`** atribut disetel ke https://aws.amazon.com/SAML/Attributes/:Domain PrincipalTag (opsional) - Elemen ini berisi satu elemen `AttributeValue` yang menyediakan nama domain yang sepenuhnya memenuhi syarat DNS Direktori Aktif (FQDN) untuk pengguna yang masuk. Parameter ini digunakan dengan otentikasi berbasis sertifikat ketika Active Directory `userPrincipalName` untuk pengguna berisi akhiran alternatif. Nilai harus disediakan di`domain.com`, termasuk subdomain apa pun.
- **`Attribute`**elemen dengan **`Name`** atribut diatur ke https://aws.amazon.com/SAML/Attributes/SessionDuration (opsional) - Elemen ini berisi satu `AttributeValue` elemen yang menentukan jumlah maksimum waktu bahwa sesi streaming federasi untuk pengguna dapat tetap aktif sebelum otentikasi ulang diperlukan. Default-nya adalah 3600 detik (60 menit). Untuk informasi lebih lanjut, lihat SAMP `SessionDurationAttribute`.

> **Note**
>
> Meskipun `SessionDuration` merupakan atribut opsional, kami sarankan Anda memasukkannya ke dalam respons SAMP. Jika Anda tidak menentukan atribut ini, durasi sesi diatur ke nilai default 3600 detik (60 menit). WorkSpaces sesi desktop terputus setelah durasi sesi berakhir.

Untuk informasi selengkapnya tentang cara mengonfigurasi elemen-elemen ini, lihat Mengonfigurasi pernyataan SAMP untuk respons autentikasi di Panduan Pengguna IAM. Untuk informasi tentang persyaratan konfigurasi khusus untuk IDP Anda, lihat dokumentasi IDP Anda.

Langkah 6: Konfigurasikan status relay federasi Anda

Selanjutnya, gunakan IDP Anda untuk mengonfigurasi status relai federasi Anda untuk menunjuk ke URL status relai WorkSpaces direktori. Setelah otentikasi berhasil olehAWS, pengguna diarahkan ke titik akhir WorkSpaces direktori, didefinisikan sebagai status relai dalam respons otentikasi SAMP.

Berikut ini adalah format URL status relai:

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

Buat URL status relai Anda dari kode registrasi WorkSpaces direktori Anda dan titik akhir status relai yang terkait dengan Wilayah tempat direktori Anda berada. Kode pendaftaran dapat ditemukan di konsol WorkSpaces manajemen.

Secara opsional, jika Anda menggunakan pengalihan lintas wilayah WorkSpaces, Anda dapat mengganti kode registrasi dengan nama domain yang memenuhi syarat penuh (FQDN) yang terkait dengan direktori di Wilayah utama dan failover Anda. Untuk informasi selengkapnya, lihat Pengalihan lintas wilayah untuk Amazon. WorkSpaces Saat menggunakan pengalihan lintas wilayah dan otentikasi SAMP 2.0, direktori primer dan failover harus diaktifkan untuk otentikasi SAMP 2.0 dan dikonfigurasi secara independen dengan iDP, menggunakan titik akhir status relai yang terkait dengan setiap Wilayah. Ini akan memungkinkan FQDN untuk dikonfigurasi dengan benar ketika pengguna mendaftarkan aplikasi WorkSpaces klien mereka sebelum masuk, dan akan memungkinkan pengguna untuk mengautentikasi selama peristiwa failover.

Tabel berikut mencantumkan titik akhir status relai untuk Wilayah tempat otentikasi WorkSpaces SAMP 2.0 tersedia.

Wilayah di mana otentikasi WorkSpaces SAMP 2.0 tersedia

Wilayah	Titik akhir status relai
Wilayah AS Timur (Virginia Utara)	• ruang kerja.euc-sso.us-east-1.aws.amazon.com

Wilayah	Titik akhir status relai
	• (FIPS) ruang kerja. euc-sso-fips.us-east-1.aws.amazon.com
Wilayah AS Barat (Oregon)	• ruang kerja.euc-sso.us-west-2.aws.amazon.com • (FIPS) ruang kerja. euc-sso-fips.us-west-2.aws.amazon.com
Wilayah Afrika (Cape Town)	ruang kerja.euc-sso.af-south-1.aws.amazon.com
Wilayah Asia Pasifik (Mumbai)	ruang kerja.euc-sso.ap-south-1.aws.amazon.com
Wilayah Asia Pasifik (Seoul)	ruang kerja.euc-sso.ap-northeast-2.aws.amazon.com
Wilayah Asia Pasifik (Singapura)	ruang kerja.euc-sso.ap-southeast-1.aws.amazon.com
Wilayah Asia Pasifik (Sydney)	ruang kerja.euc-sso.ap-southeast-2.aws.amazon.com
Wilayah Asia Pasifik (Tokyo)	ruang kerja.euc-sso.ap-northeast-1.aws.amazon.com
Wilayah Kanada (Pusat)	ruang kerja.euc-sso.ca-central-1.aws.amazon.com
Wilayah Eropa (Frankfurt)	ruang kerja.euc-sso.eu-central-1.aws.amazon.com
Wilayah Eropa (Irlandia)	ruang kerja.euc-sso.eu-west-1.aws.amazon.com
Wilayah Eropa (London)	ruang kerja.euc-sso.eu-west-2.aws.amazon.com

Wilayah	Titik akhir status relai
Wilayah Amerika Selatan (Sao Paulo)	ruang kerja.euc-sso.sa-east-1.aws.amazon.com
Wilayah Israel (Tel Aviv)	ruang kerja.euc-sso.il-central-1.aws.amazon.com
AWS GovCloud (AS-Barat)	• ruang kerja.euc-sso. us-gov-west-1. amazonaws-us-gov.com • (FIPS) ruang kerja. euc-sso-fips. us-gov-west-1. amazonaws-us-gov.com **Note** Untuk informasi selengkapnya, lihat Amazon WorkSpaces di Panduan Pengguna AWS GovCloud (AS).
AWS GovCloud (AS-Timur)	• ruang kerja.euc-sso. us-gov-east-1. amazonaws-us-gov.com • (FIPS) ruang kerja. euc-sso-fips. us-gov-east-1. amazonaws-us-gov.com **Note** Untuk informasi selengkapnya, lihat Amazon WorkSpaces di Panduan Pengguna AWS GovCloud (AS).

Langkah 7: Aktifkan integrasi dengan SAMP 2.0 di direktori Anda WorkSpaces

Anda dapat menggunakan WorkSpaces konsol untuk mengaktifkan otentikasi SAMP 2.0 pada direktori. WorkSpaces

Untuk mengaktifkan integrasi dengan SAMP 2.0

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih pada ID Direktori untuk Anda WorkSpaces.
4. Di bawah Otentikasi, pilih Edit.
5. Pilih Edit Penyedia Identitas SAMP 2.0.
6. Periksa Aktifkan otentikasi SAMP 2.0.
7. Untuk URL Akses Pengguna dan nama parameter tautan dalam IDP, masukkan nilai yang berlaku untuk IDP Anda dan aplikasi yang telah Anda konfigurasikan di Langkah 1. Nilai default untuk nama parameter deep link idP adalah RelayState “jika Anda menghilangkan parameter ini. Tabel berikut mencantumkan URL akses pengguna dan nama parameter yang unik untuk berbagai penyedia identitas untuk aplikasi.

   Domain dan alamat IP untuk ditambahkan ke daftar izin Anda

Penyedia identitas	Parameter	URL akses pengguna
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>`
Duo Masuk Tunggal	`RelayState`	`https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso`
Okta	`RelayState`	`https://<sub_domain>.okta.com/app/<a`

Penyedia identitas	Parameter	URL akses pengguna
		`pp_name>/<app_id>/sso/saml`
OneLogin	`RelayState`	`https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>`
PingFederate	`TargetResource`	`https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>`
PingOne untuk Enterprise	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>`

URL akses pengguna biasanya ditentukan oleh penyedia untuk SSO yang diprakarsai IDP yang tidak diminta. Seorang pengguna dapat memasukkan URL ini di browser web untuk federasi langsung ke aplikasi SAMP. Untuk menguji URL akses pengguna dan nilai parameter untuk IDP Anda, pilih Uji. Salin dan tempel URL pengujian ke jendela pribadi di browser Anda saat ini atau browser lain untuk menguji login SAMP 2.0 tanpa mengganggu sesi konsol AWS manajemen Anda saat ini. Ketika alur yang dimulai IDP terbuka, Anda dapat mendaftarkan klien Anda. WorkSpaces Untuk informasi selengkapnya, lihat Alur yang dimulai oleh penyedia identitas (IDP).

8. Kelola pengaturan fallback dengan mencentang atau menghapus centang Izinkan klien yang tidak mendukung SAMP 2.0 untuk masuk. Aktifkan pengaturan ini untuk terus memberikan pengguna Anda akses untuk WorkSpaces menggunakan jenis klien atau versi yang tidak mendukung SAMP 2.0 atau jika pengguna perlu waktu untuk meningkatkan ke versi klien terbaru.

> **Note**
>
> Pengaturan ini memungkinkan pengguna untuk melewati SAMP 2.0 dan masuk menggunakan otentikasi direktori menggunakan versi klien yang lebih lama.

9. Untuk menggunakan SAMP dengan klien web, aktifkan Akses Web. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasi Akses WorkSpaces Web Amazon.

> **Note**
>
> PCoIP dengan SAMP tidak didukung pada Akses Web.

10. Pilih Simpan. WorkSpaces Direktori Anda sekarang diaktifkan dengan integrasi SAMP 2.0. Anda dapat menggunakan alur yang diprakarsai oleh IDP dan yang dimulai aplikasi klien untuk mendaftarkan aplikasi WorkSpaces klien dan masuk. WorkSpaces

Otentikasi berbasis sertifikat

Anda dapat menggunakan otentikasi berbasis sertifikat WorkSpaces untuk menghapus prompt pengguna untuk kata sandi domain Active Directory. Dengan menggunakan otentikasi berbasis sertifikat dengan domain Active Directory, Anda dapat:

- Andalkan penyedia identitas SAMP 2.0 Anda untuk mengautentikasi pengguna dan memberikan pernyataan SAMP agar sesuai dengan pengguna di Active Directory.
- Aktifkan pengalaman masuk masuk tunggal dengan lebih sedikit permintaan pengguna.
- Aktifkan alur otentikasi tanpa kata sandi menggunakan penyedia identitas SAMP 2.0 Anda.

Otentikasi berbasis sertifikat menggunakan AWS Private CA sumber daya di akun Anda. AWS AWS Private CAmemungkinkan pembuatan hierarki otoritas sertifikat pribadi (CA), termasuk CA root dan bawahan. DenganAWS Private CA, Anda dapat membuat hierarki CA Anda sendiri dan mengeluarkan sertifikat dengannya untuk mengautentikasi pengguna internal. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Private Certificate Authority.

Saat menggunakan AWS Private CA untuk otentikasi berbasis sertifikat, WorkSpaces akan meminta sertifikat untuk pengguna Anda secara otomatis selama otentikasi sesi. Pengguna diautentikasi ke Active Directory menggunakan kartu pintar virtual yang disediakan dengan sertifikat.

Otentikasi berbasis sertifikat didukung dengan bundel Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) menggunakan aplikasi klien Akses WorkSpaces Web, Windows, dan macOS terbaru. Buka unduhan WorkSpaces Klien Amazon untuk menemukan versi terbaru:

- Klien Windows versi 5.5.0 atau yang lebih baru
- klien macOS versi 5.6.0 atau yang lebih baru

Untuk informasi selengkapnya tentang mengonfigurasi autentikasi berbasis sertifikat dengan Amazon WorkSpaces, lihat Cara mengonfigurasi otentikasi berbasis sertifikat untuk Amazon dan pertimbangan Desain di lingkungan yang sangat diatur untuk Otentikasi Berbasis Sertifikat dengan 2.0 WorkSpaces dan. AppStream WorkSpaces

Prasyarat

Selesaikan langkah-langkah berikut sebelum mengaktifkan otentikasi berbasis sertifikat.

1. Konfigurasikan WorkSpaces direktori Anda dengan integrasi SAMP 2.0 untuk menggunakan otentikasi berbasis sertifikat. Untuk informasi selengkapnya, lihat WorkSpacesIntegrasi dengan SAMP 2.0.
2. Konfigurasikan `userPrincipalName` atribut dalam pernyataan SAMP Anda. Untuk informasi selengkapnya, lihat Membuat Pernyataan untuk Respons Otentikasi SAMP.
3. Konfigurasikan `0bjectSid` atribut dalam pernyataan SAMP Anda. Ini opsional untuk melakukan pemetaan yang kuat ke pengguna Active Directory. Otentikasi berbasis sertifikat akan gagal jika atribut tidak cocok dengan pengenal keamanan Direktori Aktif (SID) untuk pengguna yang ditentukan dalam SAML_subject. `NameID` Untuk informasi selengkapnya, lihat Membuat Pernyataan untuk Respons Otentikasi SAMP.
4. Tambahkan TagSession izin sts: ke kebijakan kepercayaan peran IAM Anda yang digunakan dengan konfigurasi SAMP 2.0 Anda jika belum ada. Izin ini diperlukan untuk menggunakan otentikasi berbasis sertifikat. Untuk informasi selengkapnya, lihat Membuat Peran IAM Federasi SAMP 2.0.
5. Buat otoritas sertifikat pribadi (CA) menggunakan AWS Private CA jika Anda tidak memiliki satu yang dikonfigurasi dengan Active Directory Anda. AWS Private CAdiperlukan untuk menggunakan otentikasi berbasis sertifikat. Untuk informasi selengkapnya, lihat Merencanakan AWS Private CA penerapan Anda dan ikuti panduan untuk mengonfigurasi CA untuk otentikasi berbasis sertifikat. AWS Private CAPengaturan berikut adalah yang paling umum untuk kasus penggunaan otentikasi berbasis sertifikat:

a. Opsi tipe CA:

   i. Mode penggunaan CA sertifikat berumur pendek (disarankan jika Anda hanya menggunakan CA untuk menerbitkan sertifikat pengguna akhir untuk otentikasi berbasis sertifikat)

   ii. Hirarki tingkat tunggal dengan Root CA (sebagai alternatif, pilih CA bawahan jika Anda ingin mengintegrasikan dengan hierarki CA yang ada)

b. Opsi algoritma utama: RSA 2048

c. Opsi nama yang dibedakan subjek: Gunakan kombinasi opsi apa pun untuk mengidentifikasi CA di toko Otoritas Sertifikasi Root Tepercaya Direktori Aktif Anda.

d. Opsi pencabutan sertifikat: Distribusi CRL

> **Note**
>
> Otentikasi berbasis sertifikat memerlukan titik distribusi CRL online yang dapat diakses dari desktop dan pengontrol domain. Ini memerlukan akses tidak terautentikasi ke bucket Amazon S3 yang dikonfigurasi untuk entri Private CA CRL, atau distribusi CloudFront yang akan memiliki akses ke bucket S3 jika memblokir akses publik. Untuk informasi selengkapnya tentang opsi ini, lihat Merencanakan daftar pencabutan sertifikat (CRL).

6. Tandai CA pribadi Anda dengan kunci yang berhak menunjuk CA `euc-private-ca` untuk digunakan dengan otentikasi berbasis sertifikat EUC. Kuncinya tidak membutuhkan nilai. Untuk informasi selengkapnya, lihat Mengelola tag untuk CA pribadi Anda.

7. Otentikasi berbasis sertifikat menggunakan kartu pintar virtual untuk logon. Mengikuti Pedoman untuk mengaktifkan logon kartu pintar dengan otoritas sertifikasi pihak ketiga di Active Directory, lakukan langkah-langkah berikut:

   - Konfigurasikan pengontrol domain dengan sertifikat pengontrol domain untuk mengautentikasi pengguna kartu pintar. Jika Anda memiliki CA perusahaan Layanan Sertifikat Direktori Aktif yang dikonfigurasi di Direktori Aktif Anda, pengontrol domain secara otomatis terdaftar dengan sertifikat untuk mengaktifkan logon kartu pintar. Jika Anda tidak memiliki Layanan Sertifikat Direktori Aktif, lihat Persyaratan untuk sertifikat pengontrol domain dari CA pihak ketiga. Anda dapat membuat sertifikat pengontrol domain denganAWS Private CA. Jika Anda melakukan ini, jangan gunakan CA pribadi yang dikonfigurasi untuk sertifikat berumur pendek.

> **Note**
>
> Jika Anda menggunakanAWS Managed Microsoft AD, Anda dapat mengonfigurasi Layanan Sertifikat pada instans EC2 untuk memenuhi persyaratan sertifikat pengontrol domain. Lihat AWS Launch Wizardmisalnya penerapan yang AWS Managed Microsoft AD dikonfigurasi dengan Layanan Sertifikat Direktori Aktif. AWS Private CA dapat dikonfigurasi sebagai bawahan dari Active Directory Certificate Services CA, atau dapat dikonfigurasi sebagai root sendiri saat menggunakanAWS Managed Microsoft AD. Tugas konfigurasi tambahan dengan AWS Managed Microsoft AD dan Layanan Sertifikat Direktori Aktif adalah membuat aturan keluar dari grup keamanan VPC pengontrol ke instans EC2 yang menjalankan Layanan Sertifikat yang memungkinkan port TCP 135 dan 49152-65535 untuk mengaktifkan pendaftaran otomatis sertifikat. Selain itu, instans EC2 yang berjalan harus memungkinkan akses masuk pada port yang sama dari instance domain, termasuk pengontrol domain. Untuk informasi selengkapnya tentang menemukan grup keamanan untuk AWS Managed Microsoft AD lihat Mengonfigurasi subnet VPC dan grup keamanan Anda.

- Di AWS Private CA konsol atau menggunakan SDK atau CLI, pilih CA Anda dan di bawah sertifikat CA, ekspor sertifikat pribadi CA. Untuk informasi selengkapnya, lihat Mengekspor sertifikat pribadi.
- Publikasikan CA ke Active Directory. Logon ke pengontrol domain atau mesin yang bergabung dengan domain. Salin sertifikat pribadi CA ke salah satu `<path>\<file>` dan jalankan perintah berikut sebagai administrator domain. Atau, Anda dapat menggunakan Kebijakan Grup dan alat Microsoft PKI Health Tool (PKIView) untuk mempublikasikan CA. Untuk informasi selengkapnya, lihat Petunjuk konfigurasi.

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f  <path>\<file> NTAuthCA
```

Pastikan bahwa perintah berhasil diselesaikan, dan kemudian hapus file sertifikat pribadi. Bergantung pada pengaturan replikasi Active Directory, diperlukan beberapa menit agar CA dipublikasikan ke pengontrol domain dan instans desktop Anda.

> **Note**
>
> - Diperlukan bahwa Active Directory mendistribusikan CA ke Otoritas Sertifikasi Root Tepercaya dan Enterprise NTAuth menyimpan secara otomatis untuk WorkSpaces desktop ketika mereka bergabung ke domain.
> - Pengontrol domain Active Directory harus dalam mode Kompatibilitas untuk penegakan sertifikat yang kuat guna mendukung otentikasi berbasis sertifikat. Untuk informasi selengkapnya, lihat KB5014754—Perubahan autentikasi berbasis sertifikat pada pengontrol domain Windows di dokumentasi Dukungan Microsoft. Jika Anda menggunakan Microsoft AD yang AWS Dikelola, lihat Mengkonfigurasi pengaturan keamanan direktori untuk informasi selengkapnya.

Aktifkan otentikasi berbasis sertifikat

Selesaikan langkah-langkah berikut untuk mengaktifkan otentikasi berbasis sertifikat.

1. Buka WorkSpaces konsol dihttps://console.aws.amazon.com/workspaces.
2. Di panel navigasi, pilih Direktori.
3. Pilih ID Direktori untuk Anda WorkSpaces.
4. Di bawah Otentikasi, klik Edit.
5. Klik Edit Otentikasi Berbasis Sertifikat.
6. Periksa Aktifkan Otentikasi Berbasis Sertifikat.
7. Konfirmasikan bahwa CA ARN pribadi Anda terkait dalam daftar. CA pribadi harus berada di AWS akun yang sama danWilayah AWS, dan harus ditandai dengan kunci yang euc-private-ca berhak muncul dalam daftar.
8. Klik Simpan perubahan. Otentikasi berbasis sertifikat sekarang diaktifkan.
9. Reboot bundel Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) Anda agar perubahan diterapkan. Untuk informasi selengkapnya, lihat Reboot a WorkSpace.
10. Setelah reboot, ketika pengguna mengautentikasi melalui SAMP 2.0 menggunakan klien yang didukung, mereka tidak akan lagi menerima prompt untuk kata sandi domain.

> **Note**
>
> Ketika otentikasi berbasis sertifikat diaktifkan untuk masuk WorkSpaces, pengguna tidak diminta untuk otentikasi multi-faktor (MFA) bahkan jika diaktifkan pada Direktori. Saat menggunakan otentikasi berbasis sertifikat, MFA dapat diaktifkan melalui penyedia identitas SAMP 2.0 Anda. Untuk informasi selengkapnya tentang AWS Directory Service MFA, lihat Autentikasi multi-faktor (AD Connector) atau Aktifkan otentikasi multi-faktor untuk. AWS Managed Microsoft AD

Kelola otentikasi berbasis sertifikat

sertifikat CA

Dalam konfigurasi tipikal, sertifikat CA pribadi memiliki masa berlaku 10 tahun. Lihat Mengelola siklus hidup CA pribadi untuk informasi selengkapnya tentang mengganti CA dengan sertifikat kedaluwarsa, atau menerbitkan kembali CA dengan masa berlaku baru.

Sertifikat Pengguna Akhir

Sertifikat pengguna akhir yang dikeluarkan oleh AWS Private CA untuk otentikasi WorkSpaces berbasis sertifikat tidak memerlukan perpanjangan atau pencabutan. Sertifikat ini berumur pendek. WorkSpacessecara otomatis mengeluarkan sertifikat baru setiap 24 jam. Sertifikat pengguna akhir ini memiliki masa berlaku yang lebih pendek daripada distribusi AWS Private CA CRL biasa. Akibatnya, sertifikat pengguna akhir tidak perlu dicabut dan tidak akan muncul di CRL.

Laporan Audit

Anda dapat membuat laporan audit untuk mencantumkan semua sertifikat yang telah dikeluarkan atau dicabut oleh CA privat Anda. Untuk informasi selengkapnya, lihat Menggunakan laporan audit dengan CA pribadi Anda.

Pencatatan dan Pemantauan

Anda dapat menggunakan AWS CloudTrailuntuk merekam panggilan API ke AWS Private CA by WorkSpaces. Untuk informasi selengkapnya, lihat Menggunakan CloudTrail. Dalam riwayat CloudTrail acara, Anda dapat melihat `GetCertificate` dan nama `IssueCertificate` acara dari sumber `acm-pca.amazonaws.com` acara yang dibuat oleh nama WorkSpaces `EcmAssumeRoleSession` pengguna. Peristiwa ini akan direkam untuk setiap permintaan otentikasi berbasis sertifikat EUC.

Gunakan kartu pintar untuk autentikasi

Bundel Windows dan Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) memungkinkan penggunaan kartu pintar Common Access Card (CAC) dan Personal Identity Verification (PIV) untuk otentikasi.

Amazon WorkSpaces mendukung penggunaan kartu pintar untuk otentikasi pra-sesi dan otentikasi dalam sesi. Otentikasi pra-sesi mengacu pada otentikasi kartu pintar yang dilakukan saat pengguna masuk ke kartu mereka. WorkSpaces Autentikasi dalam sesi mengacu pada autentikasi yang dilakukan setelah masuk.

Misalnya, pengguna dapat menggunakan kartu pintar untuk autentikasi dalam sesi saat bekerja dengan web peramban dan aplikasi. Mereka juga dapat menggunakan kartu pintar untuk tindakan yang memerlukan izin administratif. Misalnya, jika pengguna memiliki izin administratif di Linux mereka WorkSpace, mereka dapat menggunakan kartu pintar untuk mengautentikasi diri mereka sendiri saat menjalankan `sudo` dan `sudo -i` perintah.

Daftar Isi

Persyaratan

- Direktori Konektor Direktori Aktif (AD Connector) diperlukan untuk autentikasi pra-sesi. AD Connector menggunakan autentikasi Keamanan Lapisan Pengangkutan berbasis sertifikat (mutual TLS) untuk mengautentikasi pengguna ke Direktori Aktif menggunakan sertifikat kartu pintar berbasis perangkat keras atau perangkat lunak. Untuk informasi selengkapnya tentang cara mengonfigurasi AD Connector dan direktori on-premise Anda, lihat Konfigurasi Direktori.
- Untuk menggunakan kartu pintar dengan Windows atau Linux WorkSpace, pengguna harus menggunakan klien Amazon WorkSpaces Windows versi 3.1.1 atau yang lebih baru atau klien WorkSpaces macOS versi 3.1.5 atau yang lebih baru. Untuk informasi selengkapnya tentang penggunaan kartu pintar dengan klien Windows dan macOS, lihat Dukungan Kartu Cerdas di WorkSpaces Panduan Pengguna Amazon.

- CA root dan sertifikat kartu pintar harus memenuhi persyaratan tertentu. Untuk informasi selengkapnya, lihat Mengaktifkan autentikasi mTLS di AD Connector untuk digunakan dengan kartu pintar di Panduan AWS Directory Service Administrasi dan Persyaratan Sertifikat dalam dokumentasi Microsoft.

  Selain persyaratan tersebut, sertifikat pengguna yang digunakan untuk otentikasi kartu pintar ke Amazon WorkSpaces harus menyertakan atribut berikut:

  - Pengguna AD userPrincipalName (UPN) di bidang subjectAltName (SAN) sertifikat. Kami merekomendasikan penerbitan sertifikat kartu pintar untuk UPN default pengguna.
  - Autentikasi klien (1.3.6.1.5.5.7.3.2) atribut Atribut Extended Key Usage (EKU).
  - Logon Kartu Pintar (1.3.6.1.4.1.311.20.2.2) atribut EKU.
- Untuk autentikasi pra-sesi, Online Certificate Status Protocol (OCSP) diperlukan untuk memeriksa sertifikat pencabutan. Untuk autentikasi dalam sesi, OCSP direkomendasikan, tetapi tidak diperlukan.

Batasan

- Hanya aplikasi klien WorkSpaces Windows versi 3.1.1 atau yang lebih baru dan aplikasi klien macOS versi 3.1.5 atau yang lebih baru saat ini didukung untuk otentikasi kartu pintar.
- Aplikasi klien WorkSpaces Windows 3.1.1 atau yang lebih baru mendukung kartu pintar hanya ketika klien berjalan pada versi Windows 64-bit.
- Ubuntu saat ini WorkSpaces tidak mendukung otentikasi kartu pintar.
- Hanya direktori AD Connector yang saat ini didukung untuk autentikasi kartu pintar.
- Autentikasi dalam sesi tersedia di semua Wilayah tempat WSP didukung. Autentikasi pra-sesi tersedia di Wilayah berikut:
  - Wilayah Asia Pasifik (Sydney)
  - Wilayah Asia Pacific (Tokyo)
  - Wilayah Eropa (Irlandia)
  - AWS GovCloud Wilayah (AS-Timur)
  - AWS GovCloud Wilayah (AS-Barat)
  - Wilayah AS Timur (Virginia Utara)
  - Wilayah AS Barat (Oregon)

- Untuk otentikasi dalam sesi dan otentikasi pra-sesi di Linux atau Windows WorkSpaces, hanya satu kartu pintar yang saat ini diizinkan pada satu waktu.
- Untuk otentikasi pra-sesi, mengaktifkan otentikasi kartu pintar dan otentikasi masuk pada direktori yang sama saat ini tidak didukung.
- Hanya kartu CAC dan PIV yang didukung saat ini. Tipe lain dari kartu pintar berbasis perangkat keras atau berbasis perangkat lunak mungkin juga berfungsi, tetapi belum sepenuhnya diuji untuk digunakan dengan WSP.

Konfigurasi Direktori

Untuk mengaktifkan autentikasi kartu pintar, Anda harus mengonfigurasi direktori AD Connector dan direktori on-premise Anda dengan cara berikut.

Konfigurasi direktori AD Connector

Sebelum memulai, pastikan direktori AD Connector Anda telah disiapkan seperti yang dijelaskan di Prasyarat AD Connector di Panduan Administrasi AWS Directory Service . Secara khusus, pastikan bahwa Anda telah membuka port yang diperlukan di firewall Anda.

Untuk menyelesaikan konfigurasi direktori AD Connector, ikuti petunjuk di Aktifkan autentikasi mTLS di AD Connector untuk digunakan dengan kartu pintar di Panduan AdministrasiAWS Directory Service .

> **Note**
>
> Otentikasi kartu pintar membutuhkan Kerberos Constrained Delegation (KCD) agar berfungsi dengan baik. KCD memerlukan bagian nama pengguna dari akun layanan AD Connector agar sesuai dengan SAM AccountName dari pengguna yang sama. Sebuah SAM tidak AccountName dapat melebihi 20 karakter.

Konfigurasi direktori on-premise

Selain mengonfigurasi direktori AD Connector, Anda juga harus memastikan bahwa sertifikat yang dikeluarkan untuk pengendali domain untuk direktori on-premise memiliki set extended key usage (EKU) "Autentikasi KDC". Untuk melakukannya, gunakan templat sertifikat Autentikasi Kerberos default Layanan Domain Direktori Aktif (AD DS). Jangan menggunakan templat sertifikat pengendali

Domain atau templat sertifikat autentikasi pengendali Domain karena templat tersebut tidak berisi pengaturan yang diperlukan untuk autentikasi kartu pintar.

Aktifkan kartu pintar untuk Windows WorkSpaces

Untuk panduan umum tentang cara mengaktifkan autentikasi kartu pintar pada Windows, lihat Pedoman untuk mengaktifkan kartu pintar logon dengan otoritas sertifikasi (CA) pihak ketiga dalam dokumentasi Microsoft.

Untuk mendeteksi layar kunci Windows dan memutus sesi

Untuk memungkinkan pengguna membuka kunci Windows WorkSpaces yang diaktifkan untuk otentikasi pra-sesi kartu pintar saat layar terkunci, Anda dapat mengaktifkan deteksi layar kunci Windows di sesi pengguna. Ketika layar kunci Windows terdeteksi, WorkSpace sesi terputus, dan pengguna dapat menyambung kembali dari WorkSpaces klien dengan menggunakan kartu pintar mereka.

Anda dapat mengaktifkan pemutusan sesi ketika layar kunci Windows terdeteksi dengan menggunakan pengaturan Kebijakan Grup. Untuk informasi selengkapnya, lihat Aktifkan atau nonaktifkan sesi pemutusan hubungan pada kunci layar untuk WSP.

Untuk mengaktifkan autentikasi dalam sesi atau pra-sesi

Secara default, Windows tidak WorkSpaces diaktifkan untuk mendukung penggunaan kartu pintar untuk otentikasi pra-sesi atau dalam sesi. Jika diperlukan, Anda dapat mengaktifkan otentikasi dalam sesi dan pra-sesi untuk Windows WorkSpaces dengan menggunakan pengaturan Kebijakan Grup. Untuk informasi selengkapnya, lihat Aktifkan atau nonaktifkan pengalihan kartu pintar untuk WSP.

Untuk menggunakan autentikasi pra-sesi, selain memperbarui pengaturan Kebijakan Grup, Anda juga harus mengaktifkan otentikasi pra-sesi melalui pengaturan direktori AD Connector. Untuk informasi selengkapnya, ikuti petunjuk di Aktifkan autentikasi mTLS di AD Connector untuk digunakan dalam kartu pintar di Panduan AWS Directory Service Administrasi.

Untuk mengaktifkan pengguna untuk menggunakan kartu pintar di peramban

Jika pengguna Anda menggunakan Chrome sebagai peramban mereka, tidak diperlukan konfigurasi khusus untuk menggunakan kartu pintar.

Jika pengguna Anda menggunakan Firefox sebagai peramban mereka, Anda dapat mengaktifkan pengguna Anda untuk menggunakan kartu pintar di Firefox melalui Kebijakan Grup. Anda dapat menggunakan templat Kebijakan Grup Firefox ini di GitHub.

Misalnya, Anda dapat menginstal versi 64-bit OpenSC untuk Windows untuk mendukung PKCS #11, lalu menggunakan pengaturan Kebijakan Grup berikut, saat *NAME_OF_DEVICE* adalah nilai apa pun yang ingin Anda gunakan untuk mengidentifikasi PKCS #11, seperti OpenSC, dan saat *PATH_TO_LIBRARY_FOR_DEVICE* adalah jalur ke modul PKCS #11. Jalur ini harus menuju ke pusataka dengan ekstensi .DLL, seperti `C:\Program Files\OpenSC Project\OpenSC \pkcs11\onepin-opensc-pkcs11.dll`.

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

Jika Anda menggunakan OpenSC, Anda juga dapat memuat modul `pkcs11` OpenSC ke Firefox dengan menjalankan program `pkcs11-register.exe`. Untuk menjalankan program ini, klik file dua kali pada `C:\Program Files\OpenSC Project\OpenSC\tools \pkcs11-register.exe`, atau buka jendela Command Prompt dan jalankan perintah berikut:

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

Untuk memverifikasi bahwa modul `pkcs11` OpenSC telah dimuat ke Firefox, lakukan hal berikut:

1. Jika Firefox sudah berjalan, tutup Firefox.
2. Buka Firefox. Pilih tombol menu

   Di pojok kanan atas, lalu pilih Opsi.
3. Pada halaman about:preferences, di sebelah kiri panel navigasi, pilih Privasi & Keamanan.
4. Di bawah Sertifikat, pilih Perangkat Keamanan.
5. Di kotak dialog Pengelola Perangkat, Anda akan melihat kerangka kerja kartu pintar OpenSC (0.21) di navigasi kiri, dan harus memiliki nilai berikut ketika memilihnya:

   Modul: `OpenSC smartcard framework (0.21)`

Jalan: `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

Memecahkan masalah

Untuk informasi tentang pemecahan masalah kartu pintar, lihat Masalah sertifikat dan konfigurasi dalam dokumentasi Microsoft.

Beberapa masalah umum yang dapat menyebabkan masalah:

- Pemetaan yang salah dari slot ke sertifikat.
- Memiliki beberapa sertifikat pada kartu pintar yang dapat dicocokkan dengan pengguna. Sertifikat dicocokkan menggunakan kriteria berikut:
  - CA root untuk sertifikat.
  - Bidang sertifikat <KU> dan <EKU>.
  - UPN dalam subjek sertifikat.
- Memiliki beberapa sertifikat yang memiliki `<EKU>msScLogin` dalam penggunaan kunci mereka.

Secara umum, yang terbaik adalah hanya memiliki satu sertifikat untuk autentikasi kartu pintar yang dipetakan ke slot pertama dalam kartu pintar.

Alat untuk mengelola sertifikat dan kunci pada kartu pintar (seperti menghapus atau memetakan ulang sertifikat dan kunci) mungkin khusus produsen. Untuk informasi selengkapnya, lihat dokumentasi yang disediakan oleh produsen kartu cerdas Anda.

Aktifkan kartu pintar untuk Linux WorkSpaces

Note

Linux WorkSpaces di WSP saat ini memiliki batasan sebagai berikut:

- Clipboard, audio-in, video-in, dan pengalihan zona waktu tidak didukung.
- Beberapa monitor tidak didukung.
- Anda harus menggunakan aplikasi klien WorkSpaces Windows untuk terhubung ke Linux WorkSpaces di WSP.

Untuk mengaktifkan penggunaan kartu pintar di Linux WorkSpaces, Anda harus menyertakan file sertifikat CA root dalam format PEM pada WorkSpace gambar.

Untuk mendapatkan sertifikat CA root

Anda dapat memperoleh sertifikat CA root Anda dalam beberapa cara:

- Anda dapat menggunakan sertifikat CA root yang dioperasikan oleh otoritas sertifikasi (CA) pihak ketiga.
- Anda dapat mengekspor sertifikat CA root Anda sendiri menggunakan situs Web pendaftaran, baik `http://ip_address/certsrv` atau `http://fqdn/certsrv`, saat *`ip_address`* dan *`fqdn`* adalah alamat IP dan nama domain yang memenuhi syarat (FQDN) dari server sertifikasi CA root. Untuk informasi selengkapnya tentang penggunaan situs Web pendaftaran, lihat Cara mengekspor Sertifikat Otoritas Sertifikasi (CA) akar dalam dokumentasi Microsoft.
- Anda dapat menggunakan prosedur berikut ini untuk mengekspor sertifikat CA root dari server sertifikasi CA root yang menjalankan Layanan Sertifikat Direktori Aktif (AD CS). Untuk informasi selengkapnya tentang menginstal AD CS, lihat Instal Otoritas Sertifikasi (CA) dalam dokumentasi Microsoft.

  1. Masuk ke server CA root menggunakan akun administrator.
  2. Dari menu start Windows, buka jendela prompt perintah (Mulai > Sistem Windows > Prompt Perintah).
  3. Gunakan perintah berikut untuk mengekspor sertifikat CA root ke file baru, saat *`rootca`*`.cer` adalah nama file baru:

     ```
     certutil -ca.cert rootca.cer
     ```

     Untuk informasi selengkapnya tentang menjalankan certutil, lihat certutil dalam dokumentasi Microsoft.
  4. Gunakan perintah OpenSSL berikut untuk mengonversi sertifikat CA root yang diekspor dari format DER ke format PEM, saat *`rootca`* adalah nama sertifikat. Untuk informasi selengkapnya tentang OpenSSL, lihat www.openssl.org.

     ```
     openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
     ```

Untuk menambahkan sertifikat CA root Anda ke Linux Anda WorkSpaces

Untuk membantu Anda mengaktifkan kartu pintar, kami telah menambahkan skrip `enable_smartcard` ke paket Amazon Linux WSP. Skrip tersebut melakukan tugas-tugas berikut:

- Mengimpor sertifikat CA root Anda ke basis data Layanan Keamanan Jaringan (NSS).
- Menginstal modul `pam_pkcs11` untuk Modul Autentikasi Pluggable (PAM).
- Melakukan konfigurasi default, yang mencakup pengaktifan `pkinit` selama WorkSpace penyediaan.

Prosedur berikut menjelaskan cara menggunakan `enable_smartcard` skrip untuk menambahkan sertifikat CA root Anda ke Linux Anda WorkSpaces dan untuk mengaktifkan kartu pintar untuk Linux Anda WorkSpaces.

1. Buat Linux baru WorkSpace dengan protokol WSP diaktifkan. Saat meluncurkan WorkSpace di WorkSpaces konsol Amazon, pada halaman Pilih Bundel, pastikan untuk memilih WSP untuk protokol, lalu pilih salah satu bundel publik Amazon Linux 2.
2. Pada yang baru WorkSpace, jalankan perintah berikut sebagai root, di *`pem-path`* mana jalur ke file sertifikat CA root dalam format PEM.

   ```
   /usr/lib/skylight/enable_smartcard --ca-cert pem-path
   ```

   > **Note**
   >
   > Linux WorkSpaces berasumsi bahwa sertifikat pada kartu pintar dikeluarkan untuk nama utama pengguna default pengguna (UPN), seperti*`sAMAccountName`*@*`domain`*, di mana *`domain`* adalah nama domain yang sepenuhnya memenuhi syarat (FQDN).
   > Untuk menggunakan alternatif sufiks UPN, `run /usr/lib/skylight/enable_smartcard --help` untuk informasi selengkapnya. Pemetaan alternatif untuk sufiks unik UPN untuk setiap pengguna. Oleh karena itu, pemetaan itu harus dilakukan secara individual pada setiap pengguna. WorkSpace
3. (Opsional) Secara default, semua layanan diaktifkan untuk menggunakan otentikasi kartu pintar di Linux WorkSpaces. Untuk membatasi autentikasi kartu pintar hanya untuk layanan tertentu, Anda harus mengedit `/etc/pam.d/system-auth`. Batalkan komentar pada baris `auth` untuk `pam_succeed_if.so` dan edit daftar layanan sesuai kebutuhan.

Setelah baris `auth` tidak berisi komentar, untuk mengizinkan layanan untuk menggunakan autentikasi kartu pintar, Anda harus menambahkannya ke daftar. Untuk membuat layanan hanya menggunakan autentikasi kata sandi, Anda harus menghapusnya dari daftar.

4. Lakukan penyesuaian tambahan apa pun ke. WorkSpace Misalnya, Anda mungkin ingin menambahkan kebijakan seluruh sistem ke aktifkan pengguna untuk menggunakan kartu pintar di Firefox. (Pengguna Chrome harus mengaktifkan kartu pintar pada klien mereka sendiri. Untuk informasi selengkapnya, lihat Dukungan Kartu Pintar di Panduan WorkSpaces Pengguna Amazon.)
5. Buat WorkSpace gambar khusus dan bundel dari file WorkSpace.
6. Gunakan bundel kustom baru untuk diluncurkan WorkSpaces bagi pengguna Anda.

Untuk mengaktifkan pengguna menggunakan kartu pintar di Firefox

Anda dapat mengaktifkan pengguna Anda untuk menggunakan kartu pintar di Firefox dengan menambahkan SecurityDevices kebijakan ke WorkSpace gambar Linux Anda. Untuk informasi selengkapnya tentang menambahkan kebijakan seluruh sistem ke Firefox, lihat templat kebijakan Mozilla di. GitHub

1. Pada WorkSpace yang Anda gunakan untuk membuat WorkSpace gambar Anda, buat file baru bernama `policies.json/usr/lib64/firefox/distribution/`.
2. Dalam file JSON, tambahkan SecurityDevices kebijakan berikut, di mana nilai *`NAME_OF_DEVICE`* apa pun yang ingin Anda gunakan untuk mengidentifikasi `pkcs` modul. Misalnya, Anda mungkin ingin menggunakan nilai seperti `"OpenSC"`:

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
        }
    }
}
```

Memecahkan masalah

Untuk pemecahan masalah, kami merekomendasikan untuk menambahkan utilitas `pkcs11-tools`. Utilitas ini mengizinkan Anda untuk melakukan tindakan berikut:

- Mendaftarkan setiap kartu pintar.
- Mendaftarkan slot pada setiap kartu pintar.
- Mendaftarkan sertifikat pada setiap kartu pintar.

Beberapa masalah umum yang dapat menyebabkan masalah:

- Pemetaan yang salah dari slot ke sertifikat.
- Memiliki beberapa sertifikat pada kartu pintar yang dapat dicocokkan dengan pengguna. Sertifikat dicocokkan menggunakan kriteria berikut:
  - CA root untuk sertifikat.
  - Bidang sertifikat <KU> dan <EKU>.
  - UPN dalam subjek sertifikat.
- Memiliki beberapa sertifikat yang memiliki <EKU>msScLogin dalam penggunaan kunci mereka.

Secara umum, yang terbaik adalah hanya memiliki satu sertifikat untuk autentikasi kartu pintar yang dipetakan ke slot pertama dalam kartu pintar.

Alat untuk mengelola sertifikat dan kunci pada kartu pintar (seperti menghapus atau memetakan ulang sertifikat dan kunci) mungkin khusus produsen. Alat tambahan yang dapat Anda gunakan untuk bekerja dengan kartu pintar adalah:

- `opensc-explorer`
- `opensc-tool`
- `pkcs11_inspect`
- `pkcs11_listcerts`
- `pkcs15-tool`

Untuk mengaktifkan debug pencatatan log

Untuk memecahkan masalah konfigurasi `pam_pkcs11` dan `pam-krb5`, Anda dapat mengaktifkan debug pencatatan log.

1. Dalam file `/etc/pam.d/system-auth-ac`, edit tindakan `auth` dan mengubah parameter `nodebug` dari `pam_pksc11.so` menjadi `debug`.

2. Di file `/etc/pam_pkcs11/pam_pkcs11.conf`, ubah `debug = false;` ke `debug = true;`. Opsi `debug` berlaku secara terpisah untuk setiap modul pemeta, sehingga Anda mungkin perlu untuk mengubah keduanya secara langsung di bawah bagian `pam_pkcs11` dan juga di bawah bagian pemetaan yang sesuai (secara default, adalah `mapper generic`).
3. Dalam file `/etc/pam.d/system-auth-ac`, edit tindakan `auth` dan tambahkan parameter `debug` atau `debug_sensitive` menjadi `pam_krb5.so`.

Setelah Anda mengaktifkan debug pencatatan log, sistem akan mencetak pesan debug `pam_pkcs11` langsung di terminal aktif. Pesan dari `pam_krb5` telah masuk di `/var/log/secure`.

Untuk memeriksa peta sertifikat nama pengguna kartu pintar, gunakan `pklogin_finder` perintah:

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

Saat diminta, memasukkan PIN kartu pintar. output `pklogin_finder` pada nama pengguna `stdout` pada sertifikat kartu pintar dalam formulir *`NETBIOS`*`\`*`username`*. Nama pengguna ini harus sesuai dengan nama WorkSpace pengguna.

Dalam Layanan Domain Direktori Aktif (AD DS), nama domain NetBIOS adalah nama domain pra-Windows 2000. Biasanya (tetapi tidak selalu), nama domain NetBIOS adalah subdomain nama domain Sistem Nama Domain (DNS). Misalnya, jika nama domain DNS adalah `example.com`, nama domain NetBIOS biasanya `EXAMPLE`. Jika nama domain DNS adalah `corp.example.com`, nama domain NetBIOS biasanya `CORP`.

Misalnya, untuk pengguna `mmajor` di domain `corp.example.com`, output dari `pklogin_finder` adalah `CORP\mmajor`.

> **Note**
>
> Jika Anda menerima pesan `"ERROR:pam_pkcs11.c:504: verify_certificate() failed"`, pesan ini menunjukkan bahwa `pam_pkcs11` telah menemukan sertifikat pada kartu pintar yang cocok dengan kriteria nama pengguna tetapi itu tidak mengikat sertifikat CA root yang diakui oleh mesin. Ketika itu terjadi, `pam_pkcs11` mengeluarkan pesan di atas lalu mencoba sertifikat berikutnya. Hal ini memungkinkan autentikasi hanya jika menemukan sertifikat yang keduanya cocok dengan nama pengguna dan mengikat hingga sertifikat CA akar diakui.

Untuk memecahkan masalah konfigurasi `pam_krb5`, Anda dapat secara manual memanggil `kinit` dalam mode debug dengan perintah berikut:

```
KRB5_TRACE=/dev/stdout kinit -V
```

Perintah ini harus berhasil mendapatkan Kerberos Ticket Granting Ticket (TGT). Jika gagal, coba tambahkan nama utama Kerberos yang benar secara eksplisit ke perintah. Misalnya, untuk pengguna `mmajor` di domain `corp.example.com`, gunakan perintah ini:

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

Jika perintah ini berhasil, masalahnya kemungkinan besar dalam pemetaan dari WorkSpace nama pengguna ke nama utama Kerberos. Periksa bagian `[appdefaults]/pam/mappings` dalam file `/etc/krb5.conf`.

Jika perintah ini tidak berhasil, tetapi perintah `kinit` berbasis kata sandi berhasil, periksa konfigurasi terkait `pkinit_` dalam file `/etc/krb5.conf`. Misalnya, jika kartu pintar berisi lebih dari satu sertifikat, Anda mungkin perlu melakukan perubahan pada `pkinit_cert_match`.

Menyediakan akses internet dari Anda WorkSpace

Anda WorkSpaces harus memiliki akses ke internet sehingga Anda dapat menginstal pembaruan ke sistem operasi dan menyebarkan aplikasi. Anda dapat menggunakan salah satu opsi berikut untuk memungkinkan Anda WorkSpaces di cloud pribadi virtual (VPC) mengakses internet.

Opsi

- Luncurkan WorkSpaces subnet pribadi Anda dan konfigurasikan gateway NAT di subnet publik di VPC Anda.
- Luncurkan WorkSpaces subnet publik Anda dan secara otomatis atau manual tetapkan alamat IP publik ke Anda. WorkSpaces

Untuk informasi selengkapnya tentang opsi ini, lihat bagian terkait di Konfigurasikan VPC untuk WorkSpaces.

Dengan salah satu opsi ini, Anda harus memastikan bahwa grup keamanan untuk Anda WorkSpaces memungkinkan lalu lintas keluar pada port 80 (HTTP) dan 443 (HTTPS) ke semua tujuan (`0.0.0.0/0`).

Perpustakaan ekstra Amazon Linux

Jika Anda menggunakan repositori Amazon Linux, Amazon Linux Anda harus memiliki akses internet atau Anda WorkSpaces harus mengonfigurasi titik akhir VPC ke repositori ini dan ke repositori Amazon Linux utama. Untuk informasi selengkapnya, lihat bagian Contoh: Mengaktifkan Akses ke Repositori AMI Amazon Linux di Titik akhir untuk Amazon S3. Repositori AMI Amazon Linux adalah bucket Amazon S3 di setiap Wilayah. Jika Anda ingin instans di VPC Anda untuk mengakses repositori melalui titik akhir, buat kebijakan titik akhir yang memungkinkan akses ke bucket ini. Kebijakan berikut mengizinkan akses ke repositori Amazon Linux.

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

Grup keamanan untuk Anda WorkSpaces

Ketika Anda mendaftarkan direktori dengan WorkSpaces, itu menciptakan dua grup keamanan, satu untuk pengontrol direktori dan satu lagi untuk WorkSpaces di direktori. Grup keamanan untuk WorkSpaces memiliki nama yang terdiri dari pengidentifikasi direktori diikuti oleh _controllers (misalnya, d-12345678e1_controllers). Grup keamanan untuk WorkSpaces memiliki nama yang terdiri dari pengenal direktori diikuti oleh _workspacesMembers (misalnya, D-123456FC11_WorkspacesMembers).

> **Warning**
>
> Hindari memodifikasi, menghapus, atau melepaskan _controllers dan grup keamanan _workspacesMembers. Berhati-hatilah saat memodifikasi atau menghapus grup keamanan ini, karena Anda tidak akan dapat membuat ulang grup ini dan menambahkannya kembali

setelah mereka dimodifikasi atau dihapus. Untuk informasi selengkapnya, lihat grup keamanan Amazon EC2 untuk instans Linux atau grup keamanan Amazon EC2 untuk instans Windows.

Anda dapat menambahkan grup WorkSpaces keamanan default ke direktori. Setelah Anda mengaitkan grup keamanan baru dengan WorkSpaces direktori, baru WorkSpaces yang Anda luncurkan atau WorkSpaces yang sudah ada yang Anda bangun kembali akan memiliki grup keamanan baru. Anda juga dapat menambahkan grup keamanan default baru ini ke yang ada WorkSpaces tanpa membangunnya kembali, seperti yang dijelaskan nanti dalam topik ini.

Saat Anda mengaitkan beberapa grup keamanan dengan WorkSpaces direktori, aturan dari setiap grup keamanan digabungkan secara efektif untuk membuat satu set aturan. Kami merekomendasikan agar memadatkan aturan grup keamanan Anda sedapat mungkin.

Untuk informasi selengkapnya tentang grup keamanan, lihat Grup Keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Untuk menambahkan grup keamanan ke WorkSpaces direktori

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori dan pilih Tindakan, Perbarui Detail.
4. Perluas Grup Keamanan dan pilih grup keamanan.
5. Pilih Perbarui dan Keluar.

Untuk menambahkan grup keamanan ke grup yang sudah ada WorkSpace tanpa membangunnya kembali, Anda menetapkan grup keamanan baru ke elastic network interface (ENI) dari grup keamanan. WorkSpace

Untuk menambahkan grup keamanan ke grup yang sudah ada WorkSpace

1. Temukan alamat IP untuk masing-masing WorkSpace yang perlu diperbarui.
    a. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
    b. Perluas masing-masing WorkSpace dan catat alamat WorkSpace IP-nya.
2. Temukan ENI untuk masing-masing WorkSpace dan perbarui tugas grup keamanannya.

a. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
b. Di Jaringan & Keamanan, pilih Antarmuka Jaringan.
c. Cari alamat IP pertama yang Anda catat di Langkah 1.
d. Pilih ENI yang terkait dengan alamat IP, pilih Tindakan, lalu pilih Ubah Grup Keamanan.
e. Pilih grup keamanan baru, lalu pilih Simpan.
f. Ulangi proses ini sesuai kebutuhan untuk yang lain WorkSpaces.

Grup kontrol akses IP untuk Anda WorkSpaces

Amazon WorkSpaces memungkinkan Anda mengontrol alamat IP mana yang WorkSpaces dapat Anda akses. Dengan menggunakan grup kontrol berbasis alamat IP, Anda dapat menentukan dan mengelola grup alamat IP tepercaya, dan hanya mengizinkan pengguna untuk mengakses mereka WorkSpaces ketika mereka terhubung ke jaringan tepercaya.

Grup kontrol akses IP bertindak sebagai firewall virtual yang mengontrol alamat IP dari mana pengguna diizinkan untuk mengakses mereka WorkSpaces. Untuk menentukan rentang alamat CIDR, tambahkan aturan ke grup kontrol akses IP Anda, lalu kaitkan grup dengan direktori Anda. Anda dapat mengaitkan setiap grup kontrol akses IP dengan satu direktori atau lebih. Anda dapat membuat hingga 100 grup kontrol akses IP per Wilayah per Akun AWS. Namun, Anda hanya dapat mengaitkan hingga 25 grup kontrol akses IP dengan satu direktori.

Sebuah grup kontrol akses IP default terkait dengan setiap direktori. Grup default ini menyertakan aturan default yang memungkinkan pengguna untuk mengakses mereka WorkSpaces dari mana saja. Anda tidak dapat mengubah grup kontrol akses IP default untuk direktori. Jika Anda tidak mengaitkan grup kontrol akses IP dengan direktori, grup default akan digunakan. Jika Anda mengaitkan grup kontrol akses IP dengan direktori, grup kontrol akses IP default akan dipisahkan.

Untuk menentukan alamat IP publik dan rentang alamat IP untuk jaringan terpercaya Anda, tambahkan aturan ke grup kontrol akses IP. Jika pengguna Anda mengaksesnya WorkSpaces melalui gateway NAT atau VPN, Anda harus membuat aturan yang memungkinkan lalu lintas dari alamat IP publik untuk gateway NAT atau VPN.

> **Note**
>
> - Grup kontrol akses IP tidak mengizinkan penggunaan alamat IP dinamis untuk NAT. Jika Anda menggunakan NAT, konfigurasikan NAT untuk menggunakan alamat IP statis, bukan

alamat IP dinamis. Pastikan NAT merutekan semua lalu lintas UDP melalui alamat IP statis yang sama selama sesi berlangsung. WorkSpaces

- Grup kontrol akses IP mengontrol alamat IP dari mana pengguna dapat menghubungkan sesi streaming mereka WorkSpaces. Pengguna masih dapat menjalankan fungsionalitas, seperti restart, rebuild, shutdown, dari alamat IP apa pun menggunakan API publik Amazon WorkSpaces .

Anda dapat menggunakan fitur ini dengan Akses Web, PCoIP zero clients, dan aplikasi klien untuk macOS, iPad, Windows, Chromebook, dan Android.

Buat grup kontrol akses IP

Anda dapat membuat grup kontrol akses IP sebagai berikut. Setiap grup kontrol akses IP dapat berisi hingga 10 aturan.

Untuk membuat grup kontrol akses IP

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Kontrol Akses IP.
3. Pilih Buat Grup IP.
4. Pada kotak dialog Buat Grup IP, masukkan nama dan deskripsi untuk grup dan pilih Buat.
5. Pilih grup target Anda dan pilih Edit.
6. Untuk setiap alamat IP, pilih Tambahkan Aturan. Untuk Sumber, masukkan alamat IP atau rentang alamat IP. Untuk Deskripsi, masukkan deskripsi. Jika Anda sudah selesai menambahkan aturan, pilih Simpan.

Kaitkan grup kontrol akses IP dengan direktori

Anda dapat mengaitkan grup kontrol akses IP dengan direktori untuk memastikan bahwa hanya WorkSpaces diakses dari jaringan tepercaya.

Jika Anda mengaitkan grup kontrol akses IP yang tidak memiliki aturan dengan direktori, ini memblokir semua akses ke semua WorkSpaces.

Untuk mengaitkan grup kontrol akses IP dengan direktori

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.

2. Di panel navigasi, pilih Direktori.
3. Pilih direktori dan pilih Tindakan, Detail Pembaruan.
4. Perluas Grup Kontrol Akses IP dan pilih satu atau beberapa grup kontrol akses IP.
5. Pilih Perbarui dan Keluar.

Salin grup kontrol akses IP

Anda dapat menggunakan grup kontrol akses IP yang ada sebagai dasar untuk membuat grup kontrol akses IP baru.

Untuk membuat grup kontrol akses IP dari yang sudah ada

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Kontrol Akses IP.
3. Pilih grup dan pilih Tindakan, Salin ke Baru.
4. Di kotak dialog Salin Grup IP, masukkan nama dan deskripsi untuk grup baru dan pilih Salin Grup.
5. (Opsional) Untuk mengubah aturan yang disalin dari grup asli, pilih grup baru dan pilih Edit. Tambahkan, perbarui, atau hapus aturan sesuai kebutuhan. Pilih Save (Simpan).

Menghapus grup kontrol akses IP

Anda dapat menghapus aturan dari grup kontrol akses IP kapan saja. Jika Anda menghapus aturan yang digunakan untuk mengizinkan koneksi ke a WorkSpace, pengguna terputus dari file. WorkSpace

Sebelum Anda dapat menghapus grup kontrol akses IP, Anda harus memisahkannya dari direktori apa pun.

Menghapus grup kontrol akses IP

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Untuk setiap direktori yang terkait dengan grup kontrol akses IP, pilih direktori yang terkait dan pilih Tindakan, Detail Pembaruan. Perluas Grup Kontrol Akses IP, hapus centang kotak untuk grup kontrol akses IP, dan pilih Perbarui dan Keluar.

4. Di panel navigasi, pilih Kontrol Akses IP.
5. Pilih grup dan pilih Tindakan, Hapus IP Grup.

Siapkan klien nol PCoIP untuk WorkSpaces

Klien PCoIP nol hanya kompatibel dengan WorkSpaces bundel yang menggunakan protokol PCoIP.

Jika perangkat klien nol Anda memiliki firmware versi 6.0.0 atau yang lebih baru, pengguna Anda dapat terhubung langsung ke perangkat tersebut WorkSpaces . Ketika pengguna Anda terhubung langsung ke mereka WorkSpaces menggunakan perangkat klien nol, kami sarankan menggunakan otentikasi multi-faktor (MFA) dengan direktori Anda. WorkSpaces Untuk informasi selengkapnya menggunakan MFA dengan direktori Anda, lihat dokumentasi berikut:

- AWS Managed Microsoft AD — Aktifkan autentikasi multi-faktor untuk AWS Managed Microsoft AD di Panduan Administrasi AWS Directory Service
- AD Connector — Aktifkan autentikasi multi faktor untuk AD Connector di Panduan Administrasi AWS Directory Service dan Autentikasi multi-faktor (AD Connector)
- Domain tepercaya — Aktifkan autentikasi multi-faktor untuk AWS Managed Microsoft AD di Panduan Administrasi AWS Directory Service
- Simple AD — Autentikasi multi-faktor tidak tersedia untuk Simple AD.

Pada 13 April 2021, Pengelola Hubungan PCoIP tidak lagi didukung untuk digunakan dengan versi firmware perangkat klien nol antara 4.6.0 hingga 6.0.0. Jika firmware klien nol Anda bukan versi 6.0.0 atau yang lebih baru, Anda bisa mendapatkan firmware terbaru melalui langganan Akses Desktop di https://www.teradici.com/desktop-access.

Important

- Di Antarmuka Web Adminsitrasi (Administrative Web Interface-AWI) PCoIP Teradici atau Konsol Manajemen (MC) PCoIP Teradici, pastikan Anda mengaktifkan Protokol Waktu Jaringan (Network Time Protocol-NTP). Untuk nama DNS host NTP, gunakan **`pool.ntp.org`**, dan atur port host NTP ke 123. Jika NTP tidak diaktifkan, pengguna klien nol PCoIP Anda mungkin menerima kesalahan kegagalan sertifikat, seperti "Sertifikat yang disediakan tidak valid karena stempel waktu."
- Dimulai dengan versi 20.10.4 dari agen PCoIP, Amazon WorkSpaces menonaktifkan pengalihan USB secara default melalui registri Windows. Pengaturan registri ini

memengaruhi perilaku periferal USB saat pengguna Anda menggunakan perangkat klien nol PCoIP untuk terhubung ke perangkat mereka. WorkSpaces Untuk informasi selengkapnya, lihat Printer USB dan periferal USB lainnya tidak bekerja untuk klien nol PCoIP.

Untuk informasi tentang pengaturan dan koneksi dengan perangkat klien nol PCoIP, lihat PCoIP Zero Client di Panduan Pengguna Amazon. WorkSpaces Untuk daftar perangkat klien nol PCoIP yang disetujui, lihat Klien Nol PCoIP pada situs web Teradici.

Atur Android untuk Chromebook

Versi 2.4.13 adalah rilis final dari aplikasi klien Amazon WorkSpaces Chromebook. Karena Google menghapus dukungan untuk Aplikasi Chrome secara bertahap, tidak akan ada pembaruan lebih lanjut untuk aplikasi klien WorkSpaces Chromebook, dan penggunaannya tidak didukung.

Untuk Chromebook yang mendukung pemasangan aplikasi Android, sebaiknya gunakan aplikasi klien WorkSpaces Android.

Beberapa Chromebook yang diluncurkan sebelum 2019 harus diaktifkan untuk menginstal aplikasi Android sebelum pengguna dapat menginstal aplikasi klien Amazon WorkSpaces Android. Untuk informasi selengkapnya, lihat Sistem Chrome OS yang Mendukung Aplikasi Android.

Untuk mengelola agar Chromebook pengguna Anda dapat menginstal aplikasi Android dari jarak jauh, lihat Mengatur Android di perangkat Chrome.

Aktifkan dan konfigurasikan Amazon WorkSpaces Web Access

Sebagian besar WorkSpaces bundel mendukung Amazon WorkSpaces Web Access. Untuk daftar WorkSpaces yang mendukung akses browser web, lihat “ WorkSpaces Paket Amazon mana yang mendukung Akses Web?” di Akses client, Akses Web, dan Pengalaman Pengguna.

> **Note**
>
> - Akses Web dengan WSP untuk Windows dan Ubuntu WorkSpaces didukung di semua Wilayah di mana WSP WorkSpaces tersedia. WSP untuk Amazon Linux hanya WorkSpaces tersedia di AWS GovCloud (AS-Barat).

- Kami sangat menyarankan menggunakan Akses Web dengan WSP WorkSpaces untuk kualitas streaming terbaik dan pengalaman pengguna. Berikut ini adalah batasan saat menggunakan Akses Web dengan PCoIP WorkSpaces:
  - Akses Web dengan PCoIP tidak didukung di AWS GovCloud (US) Regions, Asia Pasifik (Mumbai), Afrika (Cape Town), dan Israel (Tel Aviv)
  - Akses Web dengan PCoIP hanya didukung untuk Windows WorkSpaces, bukan dengan Amazon Linux. WorkSpaces
  - Akses Web tidak tersedia untuk beberapa Windows 10 WorkSpaces yang menggunakan protokol PCoIP. Jika PCoIP Anda WorkSpaces didukung oleh Windows Server 2019, Akses Web tidak tersedia.

Important

Mulai 1 Oktober 2020, pelanggan tidak akan lagi dapat menggunakan klien Amazon WorkSpaces Web Access untuk terhubung ke kustom Windows 7 WorkSpaces atau ke Windows 7 Bring Your Own License (BYOL) WorkSpaces.

Langkah 1: Aktifkan Akses Web ke WorkSpaces

Anda mengontrol Akses Web ke WorkSpaces tingkat direktori Anda. Untuk setiap direktori WorkSpaces yang berisi yang ingin Anda izinkan pengguna mengakses melalui klien Akses Web, lakukan langkah-langkah berikut.

Untuk mengaktifkan Akses Web ke WorkSpaces

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Di bawah kolom ID Direktori, pilih ID direktori direktori yang ingin Anda aktifkan Akses Web.
4. Pada halaman Detail Direktori, gulir ke bawah ke bagian Platform lain dan pilih Edit.
5. Pilih Akses Web.
6. Pilih Simpan.

> **Note**
>
> Setelah Anda mengaktifkan Akses Web, reboot Anda WorkSpace untuk perubahan yang akan diterapkan.

Langkah 2: Konfigurasikan akses masuk dan keluar ke port untuk Akses Web

Amazon WorkSpaces Web Access memerlukan akses masuk dan keluar untuk port tertentu. Untuk informasi selengkapnya, lihat Port untuk Web Access.

Langkah 3: Konfigurasikan kebijakan grup dan pengaturan kebijakan keamanan untuk mengizinkan pengguna untuk log on

Amazon WorkSpaces mengandalkan konfigurasi layar masuk tertentu untuk memungkinkan pengguna berhasil masuk dari klien Akses Web mereka.

Untuk mengaktifkan pengguna Akses Web untuk masuk ke mereka WorkSpaces, Anda harus mengkonfigurasi pengaturan Kebijakan Grup dan tiga pengaturan Kebijakan Keamanan. Jika pengaturan ini tidak dikonfigurasi dengan benar, pengguna mungkin mengalami waktu masuk yang lama atau layar hitam ketika mereka mencoba masuk ke pengaturan mereka WorkSpaces. Untuk mengonfigurasi pengaturan ini, gunakan prosedur berikut.

Anda dapat menggunakan Objek Kebijakan Grup (GPO) untuk menerapkan pengaturan untuk mengelola Windows WorkSpaces atau pengguna yang merupakan bagian dari WorkSpaces direktori Windows Anda. Kami menyarankan Anda membuat unit organisasi untuk Objek WorkSpaces Komputer Anda dan unit organisasi untuk Objek WorkSpaces Pengguna Anda.

Untuk informasi tentang menggunakan alat administrasi Direktori Aktif untuk bekerja dengan GPO, lihat Menginstal alat administrasi Direktori Aktif dalam Panduan Administrasi AWS Directory Service .

Untuk mengaktifkan agen WorkSpaces logon untuk beralih pengguna

Dalam kebanyakan kasus, ketika pengguna mencoba masuk ke WorkSpace, bidang nama pengguna diisi sebelumnya dengan nama pengguna tersebut. Namun, jika administrator telah membuat koneksi RDP ke WorkSpace untuk melakukan tugas pemeliharaan, bidang nama pengguna diisi dengan nama administrator sebagai gantinya.

Untuk menghindari masalah ini, nonaktifkan pengaturan Kebijakan Grup Sembunyikan titik masuk untuk Pengalihan Pengguna Cepat. Saat Anda menonaktifkan pengaturan ini, agen WorkSpaces masuk dapat menggunakan tombol Switch User untuk mengisi bidang nama pengguna dengan nama yang benar.

1. Buka alat Manajemen Kebijakan Grup (gpmc.msc) dan navigasikan ke dan pilih GPO di tingkat pengontrol domain atau domain direktori yang Anda gunakan untuk Anda WorkSpaces. (Jika Anda memiliki template administratif Kebijakan WorkSpaces Grup yang diinstal di domain Anda, Anda dapat menggunakan WorkSpaces GPO untuk akun WorkSpaces mesin Anda.)
2. Di menu utama, pilih Tindakan, pilih Edit.
3. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Sistem, dan Logon.
4. Buka pengaturan Sembunyikan titik masuk untuk Pengalihan Pengguna Cepat.
5. Di kotak dialog Sembunyikan titik masuk untuk Pengalihan Pengguna Cepat, Dinonaktifkan, lalu pilih OKE.

Untuk menyembunyikan nama pengguna yang terakhir log on

Secara default, daftar pengguna yang terakhir log on ditampilkan sebagai ganti tombol Alihkan Pengguna. Tergantung pada konfigurasi WorkSpace, daftar mungkin tidak menampilkan ubin Pengguna Lain. Ketika situasi ini terjadi, jika nama pengguna yang telah diisi sebelumnya tidak benar, agen WorkSpaces logon tidak dapat mengisi bidang dengan nama yang benar.

Untuk menghindari masalah ini, aktifkan pengaturan Kebijakan Keamanan Logon interaktif: Jangan tampilkan yang terakhir masuk atau Logon interaktif: Jangan tampilkan nama pengguna terakhir (tergantung versi Windows yang Anda gunakan).

1. Buka alat Manajemen Kebijakan Grup (gpmc.msc) dan navigasikan ke dan pilih GPO di tingkat pengontrol domain atau domain direktori yang Anda gunakan untuk Anda WorkSpaces. (Jika Anda memiliki template administratif Kebijakan WorkSpaces Grup yang diinstal di domain Anda, Anda dapat menggunakan WorkSpaces GPO untuk akun WorkSpaces mesin Anda.)
2. Di menu utama, pilih Tindakan, pilih Edit.
3. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Pengaturan Windows, Pengaturan Keamanan, Kebijakan Lokal, dan Opsi Keamanan.
4. Buka salah satu pengaturan berikut:

   - Untuk Windows 7 — Logon interaktif: Jangan tampilkan yang terakhir masuk

- Untuk Windows 10 — Logon interaktif: Jangan tampilkan nama pengguna terakhir

5. Di kotak dialog Properti untuk pengaturan, pilih Diaktifkan, lalu pilih OKE.

Untuk mengharuskan menekan CTRL+ALT+DEL sebelum pengguna dapat log on

Untuk Akses WorkSpaces Web, Anda harus mengharuskan pengguna menekan CTRL+ALT+DEL sebelum mereka dapat masuk. Mengharuskan pengguna untuk menekan CTRL+ALT+DEL sebelum mereka log on memastikan bahwa pengguna menggunakan jalur tepercaya saat memasukkan kata sandi mereka.

1. Buka alat Manajemen Kebijakan Grup (gpmc.msc) dan navigasikan ke dan pilih GPO di tingkat pengontrol domain atau domain direktori yang Anda gunakan untuk Anda WorkSpaces. (Jika Anda memiliki template administratif Kebijakan WorkSpaces Grup yang diinstal di domain Anda, Anda dapat menggunakan WorkSpaces GPO untuk akun WorkSpaces mesin Anda.)
2. Di menu utama, pilih Tindakan, pilih Edit.
3. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Pengaturan Windows, Pengaturan Keamanan, Kebijakan Lokal, dan Opsi Keamanan.
4. Buka pengaturan Logon interaktif: Tidak memerlukan pengaturan CTRL+ALT+DEL.
5. Pada tab Pengaturan Keamanan Lokal, pilih Dnonaktifkan, lalu pilih OKE.

Untuk menampilkan domain dan informasi pengguna saat sesi terkunci

Agen WorkSpaces logon mencari nama dan domain pengguna. Setelah pengaturan ini dikonfigurasi, layar kunci akan menampilkan nama lengkap pengguna (jika ditentukan dalam Direktori Aktif), nama domain mereka, dan nama pengguna mereka.

1. Buka alat Manajemen Kebijakan Grup (gpmc.msc) dan navigasikan ke dan pilih GPO di tingkat pengontrol domain atau domain direktori yang Anda gunakan untuk Anda WorkSpaces. (Jika Anda memiliki template administratif Kebijakan WorkSpaces Grup yang diinstal di domain Anda, Anda dapat menggunakan WorkSpaces GPO untuk akun WorkSpaces mesin Anda.)
2. Di menu utama, pilih Tindakan, pilih Edit.
3. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Pengaturan Windows, Pengaturan Keamanan, Kebijakan Lokal, dan Opsi Keamanan.
4. Buka pengaturan Logon interaktif: Tampilkan informasi pengguna saat sesi terkunci.

5. Pada tab Pengaturan Keamanan Lokal, pilih Nama tampilan pengguna, domain dan nama pengguna, lalu pilih OKE.

Untuk menerapkan perubahan pengaturan Kebijakan Grup dan Kebijakan Keamanan

Perubahan pengaturan Kebijakan Grup dan Kebijakan Keamanan berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup dan Kebijakan Keamanan dalam prosedur sebelumnya, lakukan salah satu hal berikut:

- Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
- Dari prompt perintah administratif, masukkan gpupdate /force.

Siapkan Amazon WorkSpaces untuk otorisasi FedRAMP atau kepatuhan DoD SRG

Untuk mematuhi Federal Risk and Authorization Management Program (FedRAMP) atau Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), Anda harus mengonfigurasi WorkSpaces Amazon untuk menggunakan enkripsi endpoint Standar Pemrosesan Informasi Federal (FIPS) di tingkat direktori. Anda juga harus menggunakan Wilayah AWS US yang memiliki otorisasi FedRAMP atau sesuai dengan DoD SRG.

Tingkat otorisasi FedRAMP (Sedang atau Tinggi) atau Tingkat Dampak DoD SRG (2, 4, atau 5) tergantung pada Wilayah AWS AS tempat Amazon digunakan. WorkSpaces Untuk tingkat otorisasi FedRAMP dan kepatuhan DoD SRG yang berlaku untuk setiap Wilayah, lihat Layanan AWS dalam Cakupan oleh Program Kepatuhan.

> **Note**
>
> Selain menggunakan enkripsi endpoint FIPS, Anda juga dapat mengenkripsi enkripsi Anda. WorkSpaces Untuk informasi selengkapnya, lihat Terenkripsi WorkSpaces.

Persyaratan

- Anda harus membuat Anda WorkSpaces di AWSWilayah AS yang memiliki otorisasi FedRAMP atau sesuai dengan DoD SRG.
- WorkSpaces Direktori harus dikonfigurasi untuk menggunakan FIPS 140-2 Validated Mode untuk enkripsi endpoint.

> **Note**
>
> Untuk menggunakan pengaturan Mode Tervalidasi FIPS 140-2, WorkSpaces direktori harus baru, atau semua yang ada WorkSpaces di direktori harus menggunakan Mode Tervalidasi FIPS 140-2 untuk enkripsi titik akhir. Jika tidak, Anda tidak dapat menggunakan pengaturan ini, dan oleh karena itu WorkSpaces yang Anda buat tidak akan mematuhi persyaratan keamanan FedRAMP atau DoD.

- Pengguna harus mengaksesnya WorkSpaces dari salah satu aplikasi WorkSpaces klien berikut:
  - Windows: 2.4.3 atau lebih baru
  - macOS: 2.4.3 atau lebih baru
  - Linux: 3.0.0 atau lebih baru
  - iOS: 2.4.1 atau lebih baru
  - Android: 2.4.1 atau lebih baru
  - Tablet Kebakaran: 2.4.1 atau yang lebih baru
  - ChromeOS: 2.4.1 atau lebih baru
  - Akses Web

Untuk menggunakan enkripsi titik akhir FIPS

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Verifikasi bahwa direktori tempat Anda ingin membuat FedRAMP-Authorized dan DoD WorkSpaces SRG-compliant tidak memiliki apa pun yang terkait dengannya. WorkSpaces Jika ada yang WorkSpaces terkait dengan direktori dan direktori belum diaktifkan untuk menggunakan FIPS 140-2 Validated Mode, baik mengakhiri WorkSpaces atau membuat direktori baru.
4. Pilih direktori yang memenuhi kriteria di atas, lalu pilih Tindakan, Perbarui Detail.

5. Pada halaman Perbarui Detail Direktori, pilih panah untuk memperluas bagian Opsi Kontrol Akses.
6. Untuk Enkripsi Titik Akhir, pilih Mode Validasi FIPS 140-2 alih-alih Mode Enkripsi TLS (Standar).
7. Pilih Perbarui dan keluar.
8. Anda sekarang dapat membuat WorkSpaces dari direktori ini yang FedRAMP resmi dan DoD SRG compliant. Untuk mengakses ini WorkSpaces, pengguna harus menggunakan salah satu aplikasi WorkSpaces klien yang tercantum sebelumnya di bagian Persyaratan.

Aktifkan koneksi SSH untuk Linux Anda WorkSpaces

Jika Anda atau pengguna Anda ingin terhubung ke Amazon Linux Anda WorkSpaces dengan menggunakan baris perintah, Anda dapat mengaktifkan koneksi SSH. Anda dapat mengaktifkan koneksi SSH ke semua WorkSpaces dalam direktori atau ke individu WorkSpaces dalam direktori.

Untuk mengaktifkan hubungan SSH, Anda membuat grup keamanan baru atau memperbarui grup keamanan yang ada dan menambahkan aturan untuk mengizinkan lalu lintas masuk untuk tujuan ini. Grup keamanan bertindak sebagai firewall untuk instans-instans yang dikaitkan, mengontrol lalu lintas ke dalam dan ke luar pada tingkat instans. Setelah Anda membuat atau memperbarui grup keamanan Anda, pengguna Anda dan orang lain dapat menggunakan PuTTY atau terminal lain untuk terhubung dari perangkat mereka ke Amazon Linux Anda. WorkSpaces Untuk informasi selengkapnya, lihat the section called “Grup keamanan”.

Untuk tutorial video, lihat Bagaimana saya bisa terhubung ke Amazon Linux saya WorkSpaces menggunakan SSH? di pusat AWS pengetahuan.

Daftar Isi

Prasyarat untuk koneksi SSH ke Amazon Linux WorkSpaces

- Mengaktifkan lalu lintas SSH masuk ke WorkSpace - Untuk menambahkan aturan untuk mengizinkan lalu lintas SSH masuk ke satu atau lebih Amazon Linux WorkSpaces, pastikan bahwa Anda memiliki alamat IP publik atau pribadi dari perangkat yang memerlukan koneksi SSH ke Anda. WorkSpaces Misalnya, Anda dapat menentukan alamat IP publik perangkat di luar virtual private cloud (VPC) atau alamat IP pribadi dari instans EC2 lain di VPC yang sama dengan VPC Anda. WorkSpace

  Jika Anda berencana untuk terhubung ke WorkSpace dari perangkat lokal Anda, Anda dapat menggunakan frasa pencarian “apa alamat IP saya” di browser internet atau menggunakan layanan berikut: Periksa IP.
- Menghubungkan ke WorkSpace - Informasi berikut diperlukan untuk memulai koneksi SSH dari perangkat ke Amazon Linux. WorkSpace
  - Nama NetBIOS domain direktori aktif yang Anda hubungkan.
  - Nama WorkSpace pengguna Anda.
  - Alamat IP publik atau pribadi WorkSpace yang ingin Anda sambungkan.

    Pribadi: Jika VPC Anda dilampirkan ke jaringan perusahaan dan Anda memiliki akses ke jaringan itu, Anda dapat menentukan alamat IP pribadi dari. WorkSpace

    Publik: Jika Anda WorkSpace memiliki alamat IP publik, Anda dapat menggunakan WorkSpaces konsol untuk menemukan alamat IP publik, seperti yang dijelaskan dalam prosedur berikut.

Untuk menemukan alamat IP untuk Amazon Linux yang ingin WorkSpace Anda sambungkan dan nama pengguna Anda

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Dalam daftar WorkSpaces, pilih WorkSpace yang ingin Anda aktifkan koneksi SSH.
4. Di kolom Running mode, konfirmasikan bahwa WorkSpace statusnya Tersedia.
5. Klik panah di sebelah kiri WorkSpace nama untuk menampilkan ringkasan sebaris, dan perhatikan informasi berikut:

   - WorkSpace IP. Ini adalah alamat IP pribadi dari WorkSpace.

Alamat IP pribadi diperlukan untuk mendapatkan elastic network interface yang terkait dengan file WorkSpace. Antarmuka jaringan diperlukan untuk mengambil informasi seperti grup keamanan atau alamat IP publik yang terkait dengan. WorkSpace

- Nama WorkSpace pengguna. Ini adalah nama pengguna yang Anda tentukan untuk terhubung ke file WorkSpace.

6. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
7. Di panel navigasi, pilih Antarmuka Jaringan.
8. Di kotak pencarian, ketik WorkSpace IP yang Anda catat di Langkah 5.
9. Pilih antarmuka jaringan yang terkait dengan WorkSpaceIP.
10. Jika Anda WorkSpace memiliki alamat IP publik, itu ditampilkan di kolom IP Publik IPv4. Catat alamat ini, jika ada.

Untuk menemukan nama NetBIOS dari domain Direktori Aktif yang terhubung dengan Anda

1. Buka AWS Directory Service konsol di https://console.aws.amazon.com/directoryservicev2/.
2. Dalam daftar direktori, klik tautan ID Direktori direktori untuk direktori. WorkSpace
3. Di bagian Detail direktori, perhatikan Nama NetBIOS Direktori.

Aktifkan koneksi SSH ke semua Amazon Linux WorkSpaces dalam sebuah direktori

Untuk mengaktifkan koneksi SSH ke semua Amazon Linux WorkSpaces dalam direktori, lakukan hal berikut.

Untuk membuat grup keamanan dengan aturan untuk mengizinkan lalu lintas SSH masuk ke semua Amazon Linux WorkSpaces dalam direktori

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, pilih Security Groups (Grup Keamanan).
3. Pilih Buat Grup Keamanan.
4. Ketik nama dan secara opsional, deskripsi untuk grup keamanan Anda.
5. Untuk VPC, pilih VPC yang berisi koneksi SSH WorkSpaces yang ingin Anda aktifkan.
6. Pada tab Masuk, pilih Tambahkan Aturan, dan lakukan hal berikut:

- Untuk Tipe, pilih SSH.
- Untuk Protokol, TCP secara otomatis ditentukan ketika Anda memilih SSH.
- Untuk Baris Port, 22 secara otomatis ditentukan saat Anda memilih SSH.
- Untuk Sumber, tentukan rentang CIDR dari alamat IP publik untuk komputer yang akan digunakan pengguna untuk terhubung ke komputer mereka WorkSpaces. Misalnya, jaringan perusahaan atau jaringan rumah.
- (Opsional) Untuk Deskripsi peran, ketik deskripsi untuk aturan.

7. Pilih Buat.

Otentikasi berbasis kata sandi di Amazon Linux 2 WorkSpaces

Amazon Linux 2 yang WorkSpaces diluncurkan sebelum 10 November 2023 mengaktifkan otentikasi kata sandi SSH secara default. Untuk Amazon Linux 2 WorkSpaces diluncurkan setelah 10 November. 2023, otentikasi kata sandi SSH dinonaktifkan secara default.

Untuk menonaktifkan otentikasi kata sandi di instans Amazon Linux 2 WorkSpaces yang ada

1. Luncurkan WorkSpaces klien dan login ke Anda WorkSpace.
2. Buka jendela Terminal (Aplikasi> Alat Sistem> Terminal MATE).
3. Di jendela Terminal, jalankan perintah berikut.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 no|' /etc/ssh/sshd_config
```

Untuk mengaktifkan otentikasi kata sandi di instans Amazon Linux 2 WorkSpaces yang baru dibuat

1. Luncurkan WorkSpaces klien dan login ke Anda WorkSpace.
2. Buka jendela Terminal (Aplikasi> Alat Sistem> Terminal MATE).
3. Di jendela Terminal, jalankan perintah berikut.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 yes|' /etc/ssh/sshd_config
```

Tidak seperti Ubuntu WorkSpaces, Amazon Linux 2 secara WorkSpaces default tidak mempertahankan pengaturan otentikasi kata sandi SSH dalam gambar khusus. Jika Anda ingin mengaktifkan otentikasi kata sandi SSH secara default di Amazon Linux 2 yang WorkSpaces

disediakan dari gambar khusus, selain mengaktifkan otentikasi kata sandi, Anda juga harus mengubah `/etc/cloud/cloud.cfg` file untuk menghapus baris yang berisi `ssh_pwauth` saat membuat gambar khusus. Untuk mengubah `/etc/cloud/cloud.cfg` file jalankan perintah berikut:

```
sudo sed -i '/^\s*ssh_pwauth:.*$/d' /etc/cloud/cloud.cfg
```

Aktifkan koneksi SSH ke Amazon Linux tertentu WorkSpace

Untuk mengaktifkan koneksi SSH ke Amazon Linux tertentu WorkSpace, lakukan hal berikut.

Untuk menambahkan aturan ke grup keamanan yang ada untuk mengizinkan lalu lintas SSH masuk ke Amazon Linux tertentu WorkSpace

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Jaringan & Keamanan, pilih Antarmuka Jaringan.
3. Di bilah pencarian, ketik alamat IP pribadi WorkSpace yang ingin Anda aktifkan koneksi SSH.
4. Di kolom Grup keamanan, klik tautan untuk grup keamanan.
5. Pada tab Masuk, pilih Edit.
6. Pilih Tambahkan aturan dan lakukan hal berikut:
   - Untuk Tipe, pilih SSH.
   - Untuk Protokol, TCP secara otomatis ditentukan ketika Anda memilih SSH.
   - Untuk Baris Port, 22 secara otomatis ditentukan saat Anda memilih SSH.
   - Untuk Sumber, pilih IP Saya atau Kustom, dan tentukan satu alamat IP atau rentang alamat IP dalam notasi CIDR. Misalnya, jika alamat IPv4 Anda adalah `203.0.113.25` tentukan `203.0.113.25/32` untuk mencantumkan alamat IPv4 tunggal ini dalam notasi CIDR. Jika perusahaan Anda mengalokasikan alamat-alamat dari rentang alamat, maka masukkan rentang alamat tersebut secara keseluruhan, seperti `203.0.113.0/24`.
   - (Opsional) Untuk Deskripsi peran, ketik deskripsi untuk aturan.
7. Pilih Simpan.

Connect ke Amazon Linux WorkSpace menggunakan Linux atau Putty

Setelah Anda membuat atau memperbarui grup keamanan Anda dan menambahkan aturan yang diperlukan, pengguna Anda dan orang lain dapat menggunakan Linux atau PuTTY untuk terhubung dari perangkat mereka ke perangkat Anda. WorkSpaces

> **Note**
>
> Sebelum menyelesaikan salah satu dari prosedur berikut, pastikan Anda memiliki yang berikut ini:
>
> - Nama NetBIOS domain direktori aktif yang Anda hubungkan.
> - Nama pengguna yang Anda gunakan untuk terhubung ke file WorkSpace.
> - Alamat IP publik atau pribadi WorkSpace yang ingin Anda sambungkan.
>
> Untuk petunjuk tentang cara mendapatkan informasi ini, lihat “Prasyarat untuk Koneksi SSH ke Amazon WorkSpaces Linux" sebelumnya dalam topik ini.

Untuk terhubung ke Amazon Linux WorkSpace menggunakan Linux

1. Buka command prompt sebagai administrator dan masukkan perintah berikut. Untuk nama *NetBIOS, Nama Pengguna*, dan *WorkSpace IP*, masukkan nilai yang berlaku.

   ```
   ssh "NetBIOS_NAME\Username"@WorkSpaceIP
   ```

   Berikut ini adalah contoh perintah SSH di mana:

   - *NetBIOS_NAME* berupa anycompany
   - *Nama pengguna* adalah janedoe
   - *WorkSpace IP* adalah 203.0.113.25

   ```
   ssh "anycompany\janedoe"@203.0.113.25
   ```

2. Saat diminta, masukkan kata sandi yang sama yang Anda gunakan saat mengautentikasi dengan WorkSpaces klien (kata sandi Direktori Aktif Anda).

Untuk terhubung ke Amazon Linux WorkSpace menggunakan PutTY

1. Buka PuTTY.
2. Di kotak dialog Konfigurasi PuTTY, lakukan hal berikut:

- Untuk Nama Host (atau alamat IP), masukkan perintah berikut. Ganti nilai dengan nama NetBIOS dari domain Active Directory yang terhubung dengan Anda, nama pengguna yang Anda gunakan untuk terhubung ke WorkSpace, dan alamat IP WorkSpace yang ingin Anda sambungkan.

  ```
  NetBIOS_NAME\Username@WorkSpaceIP
  ```

- Untuk Port, masukkan **22**.
- Untuk Tipe hubungan Pilih SSH.

Untuk contoh perintah SSH, lihat langkah 1 pada prosedur sebelumnya.

3. Pilih Buka .
4. Saat diminta, masukkan kata sandi yang sama yang Anda gunakan saat mengautentikasi dengan WorkSpaces klien (kata sandi Direktori Aktif Anda).

Konfigurasi dan komponen layanan yang diperlukan untuk WorkSpaces

Sebagai WorkSpace administrator, Anda harus memahami hal berikut tentang konfigurasi dan komponen layanan yang diperlukan.

- the section called “Konfigurasi tabel routing”
- the section called “Komponen untuk Windows”
- the section called “Komponen untuk Linux”
- the section called “Komponen untuk Ubuntu”

Konfigurasi tabel perutean yang diperlukan

Kami menyarankan Anda untuk tidak memodifikasi tabel routing tingkat sistem operasi untuk file. WorkSpace WorkSpaces Layanan ini memerlukan rute yang telah dikonfigurasi sebelumnya dalam tabel ini untuk memantau status sistem dan memperbarui komponen sistem. Jika perubahan tabel perutean diperlukan untuk organisasi Anda, hubungi AWS Support atau tim akun AWS Anda sebelum menerapkan perubahan apa pun.

Komponen layanan yang diperlukan untuk Windows

Pada Windows WorkSpaces, komponen layanan diinstal di lokasi berikut. Jangan menghapus, mengubah, memblokir, atau mengkarantina objek ini. Jika Anda melakukannya, tidak WorkSpace akan berfungsi dengan benar.

Jika perangkat lunak antivirus diinstal pada WorkSpace, pastikan tidak mengganggu komponen layanan yang diinstal di lokasi berikut.

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`
- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

Agen PCoIP 32-bit

Mulai 29 Maret 2021, kami memperbarui agen PCoIP dari 32-bit ke 64-bit. Untuk Windows WorkSpaces yang menggunakan protokol PCoIP, ini berarti bahwa lokasi file Teradici berubah dari ke. `C:\Program Files (x86)\Teradici` `C:\Program Files\Teradici` Karena kami memperbarui agen PCoIP selama jendela pemeliharaan rutin, beberapa dari Anda WorkSpaces mungkin telah menggunakan agen 32-bit lebih lama daripada yang lain selama transisi.

Jika Anda telah mengonfigurasi aturan firewall, pengecualian perangkat lunak antivirus (di sisi klien dan sisi host), pengaturan Objek Kebijakan Grup (GPO), atau pengaturan untuk Manajer Konfigurasi Pusat Sistem Microsoft (SCCM), Manajer Konfigurasi Titik Akhir Microsoft, atau manajemen konfigurasi serupa alat berdasarkan path lengkap ke agen 32-bit, Anda juga harus menambahkan jalur lengkap ke agen 64-bit ke pengaturan tersebut.

Jika Anda memfilter jalur ke komponen PCoIP 32-bit, pastikan untuk menambahkan jalur ke komponen versi 64-bit. Karena Anda WorkSpaces mungkin tidak semua diperbarui pada saat yang sama, jangan ganti jalur 32-bit dengan jalur 64-bit, atau beberapa jalur Anda WorkSpaces mungkin tidak berfungsi. Misalnya, jika Anda mendasarkan pengecualian atau filter komunikasi Anda pada `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe`, Anda juga harus menambahkan `C:\Program Files\Teradici\PCoIP Agent\bin`

`\pcoip_server.exe`. Demikian juga, jika Anda mendasarkan pengecualian atau filter komunikasi Anda `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe`, Anda juga harus menambahkan `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe`.

Perubahan layanan arbiter PCoIP - Ketahuilah bahwa layanan arbiter PCoIP (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) dihapus saat Anda diperbarui untuk menggunakan agen WorkSpaces 64-bit.

PCoIP nol klien dan perangkat USB - Dimulai dengan versi 20.10.4 dari agen PCoIP, WorkSpaces Amazon menonaktifkan pengalihan USB secara default melalui registri Windows. Pengaturan registri ini memengaruhi perilaku periferal USB saat pengguna Anda menggunakan perangkat klien nol PCoIP untuk terhubung ke perangkat mereka. WorkSpaces Untuk informasi selengkapnya, lihat Printer USB dan periferal USB lainnya tidak bekerja untuk klien nol PCoIP.

Komponen layanan yang diperlukan untuk Linux

Di Amazon Linux WorkSpaces, komponen layanan diinstal di lokasi berikut. Jangan menghapus, mengubah, memblokir, atau mengkarantina objek ini. Jika Anda melakukannya, tidak WorkSpace akan berfungsi dengan benar.

> **Note**
>
> Membuat perubahan pada file selain `/etc/pcoip-agent/pcoip-agent.conf` dapat menyebabkan Anda WorkSpaces berhenti bekerja dan mungkin mengharuskan Anda untuk membangunnya kembali. Untuk informasi tentang memodifikasi `/etc/pcoip-agent/pcoip-agent.conf`, lihat Kelola Amazon Linux Anda WorkSpaces.

- `/etc/dhcp/dhclient.conf`
- `/etc/logrotate.d/pcoip-agent`
- `/etc/logrotate.d/pcoip-server`
- `/etc/os-release`
- `/etc/pam.d/pcoip`
- `/etc/pam.d/pcoip-session`
- `/etc/pcoip-agent`
- `/etc/profile.d/system-restart-check.sh`

- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf
- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp

Komponen layanan yang diperlukan untuk Ubuntu

Di Ubuntu WorkSpaces, komponen layanan diinstal di lokasi berikut. Jangan menghapus, mengubah, memblokir, atau mengkarantina objek ini. Jika Anda melakukannya, tidak WorkSpace akan berfungsi dengan benar.

- `/etc/X11/default-display-manager`
- `/etc/X11/xorg.conf`
- `/etc/dcv`
- `/etc/default/grub.d/zz-hibernation.cfg`
- `/etc/netplan`
- `/etc/os-release`
- `/etc/pam.d/dcv`
- `/etc/pam.d/dcv-graphical-sso`
- `/etc/sssd/sssd.conf`
- `/etc/wsp`
- `/lib64/security/pam_self.so`
- `/usr/lib/skylight`
- `/usr/lib/systemd/system/dcvserver.service`
- `/usr/lib/systemd/system/dcvsessionlauncher.service`
- `/usr/lib/systemd/system/skylight-agent.service`
- `/usr/lib/systemd/system/wspdcvhostadapter.service`
- `/usr/lib/systemd/system/xdcv-console-update.service`
- `/usr/lib/systemd/system/xdcv-console.path`
- `/usr/lib/systemd/system/xdcv-console.service`
- `/usr/share/X11`
- `/var/lib/skylight`
- `/var/log/skylight`

Kelola direktori untuk WorkSpaces

WorkSpaces menggunakan direktori untuk menyimpan dan mengelola informasi untuk Anda WorkSpaces dan pengguna. Anda dapat menggunakan salah satu opsi berikut:

- AD Connector — Menggunakan Direktori Aktif Microsoft on-premise yang sudah ada. Pengguna dapat masuk WorkSpaces menggunakan kredensi lokal mereka dan mengakses sumber daya lokal dari mereka. WorkSpaces
- AWS Managed Microsoft AD — Membuat Direktori Aktif Microsoft yang di-host di AWS.
- Simple AD — Membuat direktori yang kompatibel dengan Direktori Aktif Microsoft, didukung oleh Samba 4, dan di-host di AWS.
- Kepercayaan silang — Membuat hubungan kepercayaan antara direktori AWS Managed Microsoft AD Anda dan domain on-premise.

Untuk tutorial yang menunjukkan cara mengatur direktori dan peluncuran ini WorkSpaces, lihatLuncurkan desktop virtual menggunakan WorkSpaces.

> **Tip**
>
> Untuk penjelajahan mendetail tentang pertimbangan desain direktori dan virtual private cloud (VPC) untuk berbagai skenario penerapan, lihat Praktik Terbaik untuk Menerapkan Amazon. WorkSpaces

Setelah Anda membuat direktori, Anda akan melakukan sebagian besar tugas administrasi direktori menggunakan alat bantu seperti Alat Administrasi Direktori Aktif. Anda dapat melakukan beberapa tugas administrasi direktori menggunakan WorkSpaces konsol dan tugas lain menggunakan Kebijakan Grup. Untuk informasi selengkapnya tentang mengelola pengguna dan grup, lihat Kelola WorkSpaces pengguna dan Siapkan Alat Administrasi Direktori Aktif untuk WorkSpaces.

> **Note**
>
> - Direktori bersama saat ini tidak didukung untuk digunakan dengan Amazon WorkSpaces.
> - Jika Anda mengonfigurasi direktori Microsoft AD AWS Terkelola untuk replikasi Multi-wilayah, hanya direktori di Wilayah utama yang dapat didaftarkan untuk digunakan dengan

Amazon. WorkSpaces Upaya untuk mendaftarkan direktori di Wilayah yang direplikasi untuk digunakan dengan Amazon WorkSpaces akan gagal. Replikasi Multi-Wilayah dengan AWS Microsoft AD Terkelola tidak didukung untuk digunakan dengan Amazon WorkSpaces dalam Wilayah yang direplikasi.

- Simple AD dan AD Connector tersedia untuk Anda secara gratis untuk digunakan WorkSpaces. Jika tidak ada yang WorkSpaces digunakan dengan direktori Simple AD atau AD Connector selama 30 hari berturut-turut, direktori ini akan secara otomatis dideregistrasi untuk digunakan dengan Amazon WorkSpaces, dan Anda akan dikenakan biaya untuk direktori ini sesuai ketentuan harga. AWS Directory Service

  Untuk menghapus direktori kosong, lihat Hapus direktori untuk WorkSpaces. Jika Anda menghapus direktori Simple AD atau AD Connector, Anda selalu dapat membuat yang baru ketika Anda ingin mulai menggunakan WorkSpaces lagi.

Konten

Daftarkan direktori dengan WorkSpaces

Untuk memungkinkan WorkSpaces untuk menggunakan AWS Directory Service direktori yang ada, Anda harus mendaftarkannya dengan WorkSpaces. Setelah Anda mendaftarkan direktori, Anda dapat meluncurkan WorkSpaces di direktori.

Persyaratan

Untuk mendaftarkan direktori untuk digunakan WorkSpaces, itu harus memenuhi persyaratan berikut:

- Jika Anda menggunakan AWS Managed Microsoft AD atau Simple AD, direktori Anda dapat berada di subnet pribadi khusus, selama direktori memiliki akses ke VPC tempat berada WorkSpaces .

Untuk informasi selengkapnya tentang direktori dan desain VPC, lihat whitepaper Praktik Terbaik untuk Menerapkan Amazon. WorkSpaces

> **Note**
>
> Simple AD dan AD Connector tersedia untuk Anda secara gratis untuk digunakan WorkSpaces. Jika tidak ada yang WorkSpaces digunakan dengan direktori Simple AD atau AD Connector selama 30 hari berturut-turut, direktori ini akan secara otomatis dideregistrasi untuk digunakan dengan Amazon WorkSpaces, dan Anda akan dikenakan biaya untuk direktori ini sesuai ketentuan harga. AWS Directory Service
> Untuk menghapus direktori kosong, lihat Hapus direktori untuk WorkSpaces. Jika Anda menghapus direktori Simple AD atau AD Connector, Anda selalu dapat membuat yang baru ketika Anda ingin mulai menggunakan WorkSpaces lagi.

Untuk mendaftarkan sebuah direktori

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori.
4. Pilih Tindakan, Daftar.

   > **Note**
   >
   > - Direktori bersama saat ini tidak didukung untuk digunakan dengan Amazon WorkSpaces.
   > - Jika AWS Managed Microsoft AD direktori Anda telah dikonfigurasi untuk replikasi Multi-wilayah, hanya direktori di Wilayah utama yang dapat didaftarkan untuk digunakan dengan Amazon. WorkSpaces Upaya untuk mendaftarkan direktori di Wilayah yang direplikasi untuk digunakan dengan Amazon WorkSpaces akan gagal. Replikasi Multi-Wilayah dengan AWS Managed Microsoft AD tidak didukung untuk digunakan dengan Amazon WorkSpaces dalam Wilayah yang direplikasi.

5. Pilih dua subnet VPC Anda yang bukan dari Availability Zone yang sama. Subnet ini akan digunakan untuk meluncurkan Anda WorkSpaces. Untuk informasi selengkapnya, lihat Zona Ketersediaan untuk Amazon WorkSpaces.

> **Note**
>
> Jika Anda tidak tahu subnet mana yang harus dipilih, pilih No Preference.

6. Untuk Aktifkan Izin Layanan Mandiri, pilih Ya untuk memungkinkan pengguna Anda membangun kembali WorkSpaces, mengubah ukuran volume, jenis komputasi, dan mode berjalan. Mengaktifkan dapat memengaruhi berapa banyak Anda membayar untuk Amazon WorkSpaces. Pilih Tidak jika sebaliknya.
7. Untuk Aktifkan Amazon WorkDocs, pilih Ya untuk mendaftarkan direktori untuk digunakan dengan Amazon WorkDocs atau Tidak sebaliknya.

> **Note**
>
> Opsi ini hanya ditampilkan jika Amazon WorkDocs tersedia di Wilayah dan jika Anda tidak menggunakannyaAWS Managed Microsoft AD. Jika Anda menggunakan AWS Managed Microsoft AD, selesaikan pendaftaran direktori Anda, lalu lihat Aktifkan Amazon WorkDocs untuk Microsoft AD yang AWS Dikelola.

8. Pilih Daftar. Awalnya nilai yang Terdaftar adalah `REGISTERING`. Setelah pendaftaran selesai, nilainya adalah `Yes`.

Ketika Anda selesai menggunakan direktori dengan WorkSpaces, Anda dapat membatalkan pendaftarannya. Perhatikan bahwa Anda harus membatalkan pendaftaran direktori sebelum dapat menghapusnya. Jika Anda ingin membatalkan pendaftaran dan menghapus direktori, Anda harus terlebih dahulu menemukan dan menghapus semua aplikasi serta layanan yang terdaftar ke direktori. Untuk informasi selengkapnya, lihat Hapus Direktori Anda dalam Panduan Administrasi AWS Directory Service.

Untuk membatalkan pendaftaran direktori

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori.
4. Pilih Tindakan, Batalkan Pendaftaran.
5. Ketika konfirmasi diminta, pilih Batalkan Pendaftaran. Setelah pembatalan pendaftaran selesai, nilai yang Terdaftar adalah `No`.

Perbarui detail direktori untuk WorkSpaces

Anda dapat menyelesaikan tugas manajemen direktori berikut menggunakan WorkSpaces konsol.

Tugas

- Memilih unit organisasi
- Konfigurasikan alamat IP publik otomatis
- Kendalikan akses perangkat
- Kelola izin administrator lokal
- Perbarui akun AD Connector (AD Connector)
- Autentikasi multi-faktor (AD Connector)

Memilih unit organisasi

WorkSpace akun mesin ditempatkan di unit organisasi default (OU) untuk WorkSpaces direktori. Awalnya, akun mesin ditempatkan di Komputer OU dari direktori Anda atau direktori yang terhubung ke AD Connector Anda. Anda dapat memilih OU yang berbeda dari direktori Anda atau direktori terhubung, atau menentukan OU di domain target terpisah. Perhatikan bahwa Anda hanya dapat memilih satu OU per direktori.

Setelah Anda memilih OU baru, akun mesin untuk semua WorkSpaces yang dibuat atau dibangun kembali ditempatkan di OU yang baru dipilih.

Untuk memilih unit organisasi

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda.
4. Di bawah Domain target dan unit organisasi, pilih Edit.
5. Untuk menemukan OU, di bawah Target dan unit organisasi, Anda dapat mulai mengetik semua atau sebagian dari nama OU dan memilih OU yang ingin Anda gunakan.
6. (Opsional) Pilih nama OU yang distiguished untuk menimpa OU yang Anda pilih dengan OU khusus.
7. Pilih Simpan.

8. (Opsional) Membangun kembali yang ada WorkSpaces untuk memperbarui OU. Untuk informasi selengkapnya, lihat Membangun kembali WorkSpace.

Konfigurasikan alamat IP publik otomatis

Setelah Anda mengaktifkan penetapan otomatis alamat IP publik, setiap WorkSpace yang Anda luncurkan diberi alamat IP publik dari kumpulan alamat publik yang disediakan Amazon. Sebuah WorkSpace subnet publik dapat mengakses internet melalui gateway internet jika memiliki alamat IP publik. WorkSpaces yang sudah ada sebelum Anda mengaktifkan penugasan otomatis tidak menerima alamat publik sampai Anda membangunnya kembali.

Perhatikan bahwa Anda tidak perlu mengaktifkan penetapan otomatis alamat publik jika Anda WorkSpaces berada di subnet pribadi dan Anda mengonfigurasi gateway NAT untuk virtual private cloud (VPC), atau jika Anda WorkSpaces berada di subnet publik dan Anda menetapkannya Alamat IP elastis. Untuk informasi selengkapnya, lihat Konfigurasikan VPC untuk WorkSpaces.

> **Warning**
>
> Jika Anda mengaitkan alamat IP Elastis yang Anda miliki ke sebuah WorkSpace, dan kemudian Anda kemudian memisahkan alamat IP Elastis itu dari WorkSpace, alamat IP publiknya WorkSpace kehilangan, dan itu tidak secara otomatis mendapatkan yang baru dari kumpulan yang disediakan Amazon. Untuk mengaitkan alamat IP publik baru dari kumpulan yang disediakan Amazon dengan WorkSpace, Anda harus membangun kembali. WorkSpace Jika Anda tidak ingin membangun kembali WorkSpace, Anda harus mengaitkan alamat IP Elastis lain yang Anda miliki ke alamat IP Elastic. WorkSpace

Untuk mengonfigurasi Alamat IP Elastis

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori untuk Anda WorkSpaces.
4. Pilih Tindakan, Detail Pembaruan.
5. Perluas Akses ke Internet dan pilih Aktifkan atau Nonaktifkan.
6. Pilih Perbarui.

Kendalikan akses perangkat

Anda dapat menentukan jenis perangkat yang memiliki akses ke WorkSpaces. Selain itu, Anda dapat membatasi akses WorkSpaces ke perangkat tepercaya (juga dikenal sebagai perangkat terkelola).

Untuk mengontrol akses perangkat ke WorkSpaces

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda.
4. Di bawah Opsi kontrol akses, pilih Edit.
5. Di bawah Perangkat tepercaya, tentukan jenis perangkat mana yang dapat diakses WorkSpaces dengan memilih Izinkan semua, Perangkat tepercaya, atau Tolak semua. Untuk informasi selengkapnya, lihat Batasi WorkSpaces akses ke perangkat tepercaya.
6. Pilih Simpan.

Kelola izin administrator lokal

Anda dapat menentukan apakah pengguna adalah administrator lokal pada mereka WorkSpaces, yang memungkinkan mereka untuk menginstal aplikasi dan memodifikasi pengaturan pada mereka WorkSpaces. Pengguna adalah administrator lokal secara default. Jika Anda mengubah setelan ini, perubahan berlaku untuk semua WorkSpaces yang baru yang Anda buat dan apa pun WorkSpaces yang Anda bangun kembali.

Untuk mengubah izin administrator lokal

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda.
4. Di bawah Pengaturan administrator lokal, pilih Edit.
5. Untuk memastikan bahwa pengguna adalah administrator lokal, pilih Aktifkan setelan administrator lokal.
6. Pilih Simpan.

Perbarui akun AD Connector (AD Connector)

Anda dapat memperbarui akun AD Connector yang digunakan untuk membaca pengguna dan grup dan menggabungkan akun WorkSpaces mesin ke direktori AD Connector.

Untuk memperbarui akun AD Connector

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda dan kemudian pilih Lihat detail.
4. Di bawah akun konektor AD, pilih Edit.
5. Masukkan kredensi masuk untuk akun baru.
6. Pilih Simpan.

Autentikasi multi-faktor (AD Connector)

Anda dapat mengaktifkan autentikasi multi-faktor (MFA) untuk direktori AD Connector Anda. Untuk informasi selengkapnya tentang penggunaan Autentikasi multi-faktor dengan AWS Directory Service, lihat Aktifkan autentikasi multi-faktor untuk AD Connector dan Prasyarat AD Connector.

> **Note**
>
> - Server RADIUS Anda dapat di-host oleh AWS tau dapat juga on-premise.
> - Nama pengguna harus cocok antara Direktori Aktif dengan server RADIUS Anda.

Untuk mengaktifkan autentikasi multi-faktor

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda, lalu pilih Tindakan, Detail Pembaruan.
4. Perluas Autentikasi Multi-Faktor, lalu pilih Aktifkan Autentikasi Multi-Faktor.
5. Untuk Alamat IP server RADIUS, ketik alamat IP dari titik akhir server RADIUS Anda yang dipisahkan dengan koma, atau ketik alamat IP dari penyeimbang beban server RADIUS Anda.

6. Untuk Port, ketik Port yang digunakan oleh server RADIUS Anda untuk komunikasi. Jaringan on-premise Anda harus mengizinkan lalu lintas masuk melalui port server RADIUS default (UDP:1812) dari AD Connector.
7. Untuk Kode rahasia bersama dan Konfirmasi kode rahasia bersama, ketik kode rahasia bersama untuk server RADIUS Anda.
8. Untuk Protokol, pilih protokol untuk server RADIUS Anda.
9. Untuk Waktu habis server, ketik waktu, dalam detik, untuk menunggu server RADIUS merespons. Nilai ini harus berada di antara 1 hingga 50.
10. Untuk Percobaan ulang maksimum, ketik jumlah percobaan komunikasi dengan server RADIUS. Nilai ini harus berada di antara 0 hingga 10.
11. Pilih Perbarui dan keluar.

Autentikasi multi-faktor tersedia saat Status RADIUS adalah Diaktifkan. Sementara otentikasi multi-faktor sedang disiapkan, pengguna tidak dapat masuk ke mereka. WorkSpaces

Perbarui server DNS untuk Amazon WorkSpaces

Jika Anda perlu memperbarui alamat IP server DNS untuk Active Directory Anda setelah meluncurkan WorkSpaces, Anda juga harus memperbarui WorkSpaces dengan pengaturan server DNS baru.

Anda dapat memperbarui WorkSpaces dengan pengaturan DNS baru dengan salah satu cara berikut:

- Perbarui pengaturan DNS WorkSpaces sebelum Anda memperbarui pengaturan DNS untuk Active Directory.
- Membangun kembali WorkSpaces setelah Anda memperbarui pengaturan DNS untuk Active Directory.

Sebaiknya perbarui pengaturan DNS WorkSpaces sebelum memperbarui pengaturan DNS di Active Directory (seperti yang dijelaskan pada Langkah 1 dari prosedur berikut).

Jika Anda ingin membangun kembali WorkSpaces sebagai gantinya, perbarui salah satu alamat IP server DNS di Direktori Aktif Anda (Langkah 2), lalu ikuti prosedur Membangun kembali WorkSpace untuk membangun kembali alamat Anda. WorkSpaces Setelah Anda membangun kembali WorkSpaces, ikuti prosedur di Langkah 3 untuk menguji pembaruan server DNS Anda.

Setelah menyelesaikan langkah itu, perbarui alamat IP server DNS kedua Anda di Active Directory, lalu bangun kembali. WorkSpaces Pastikan untuk mengikuti prosedur di Langkah 3 untuk menguji pembaruan server DNS kedua Anda. Sebagaimana dicatat dalam Praktik Terbaik, kami merekomendasikan memperbarui alamat IP server DNS Anda satu per satu.

Praktik terbaik

Ketika Anda memperbarui pengaturan server DNS Anda, kami merekomendasikan praktik terbaik berikut:

- Untuk menghindari pemutusan dan tidak dapat diaksesnya sumber daya domain, kami sangat merekomendasikan untuk melakukan pembaruan server DNS di luar jam sibuk atau selama periode pemeliharaan yang direncanakan.
- Jangan meluncurkan yang baru WorkSpaces selama 15 menit sebelum dan 15 menit setelah mengubah pengaturan server DNS Anda.
- Saat memperbarui pengaturan server DNS Anda, ubah satu alamat IP server DNS sekaligus. Verifikasi bahwa pembaruan pertama benar sebelum memperbarui alamat IP kedua. Kami merekomendasikan prosedur berikut (Langkah 1, Langkah 2, dan Langkah 3) dua kali untuk memperbarui alamat IP satu per satu.

Langkah 1: Perbarui pengaturan server DNS pada Anda WorkSpaces

Dalam prosedur berikut, nilai alamat IP server DNS saat ini dan yang baru disebut sebagai berikut:

- Alamat IP DNS saat ini: *`OldIP1`*, *`OldIP2`*
- Alamat IP DNS baru: *`NewIP1`*, *`NewIP2`*

> **Note**
>
> Jika ini adalah kedua kalinya Anda melakukan prosedur ini, ganti *`OldIP1`* dengan *`OldIP2`* dan *`NewIP1`* dengan *`NewIP2`*.

Perbarui pengaturan server DNS untuk Windows WorkSpaces

Jika Anda memiliki beberapa WorkSpaces, Anda dapat menyebarkan pembaruan registri berikut ke WorkSpaces dengan menerapkan Objek Kebijakan Grup (GPO) pada Active Directory OU

untuk Anda. WorkSpaces Untuk informasi selengkapnya tentang bekerja dengan GPO, lihat Kelola Windows Anda WorkSpaces.

Anda dapat melakukan pembaruan ini baik dengan menggunakan Registry Editor atau dengan menggunakan Windows PowerShell. Kedua prosedur dijelaskan di bagian ini.

Untuk memperbarui pengaturan registri DNS menggunakan Editor Registri

1. Di Windows Anda WorkSpace, buka kotak pencarian Windows, dan masukkan **`registry editor`** untuk membuka Registry Editor (regedit.exe).
2. Saat ditanya "Apakah Anda ingin mengizinkan aplikasi ini membuat perubahan pada perangkat Anda?", pilih Ya.
3. Di Editor Registri, arahkan ke entri registri berikut:

   HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Amazon\ SkyLight
4. Buka kunci DomainJoinDnsregistri. Perbarui *`OldIP1`* dengan *`NewIP1`*, lalu pilih OKE.
5. Tutup Editor Registri.
6. Reboot WorkSpace, atau restart layanan SkyLightWorkspaceConfigService.

   > **Note**
   >
   > Setelah Anda me-restart layanan SkyLightWorkspaceConfigService, dapat memakan waktu hingga 1 menit untuk adaptor jaringan untuk mencerminkan perubahan.
7. Lanjutkan ke Langkah 2, dan perbarui pengaturan server DNS Anda di Direktori Aktif untuk menggantikan *`OldIP1`* dengan *`NewIP1`*.

Untuk memperbarui pengaturan registri DNS menggunakan PowerShell

Prosedur berikut menggunakan PowerShell perintah untuk memperbarui registri Anda dan memulai ulang layanan SkyLightWorkspaceConfigService.

1. Di Windows Anda WorkSpace, buka kotak pencarian Windows, dan masukkan**`powershell`**. Pilih Jalankan sebagai Administrator.
2. Saat ditanya "Apakah Anda ingin mengizinkan aplikasi ini melakukan perubahan pada perangkat?", PilihYa.
3. Di PowerShell jendela, jalankan perintah berikut untuk mengambil alamat IP server DNS saat ini.

```
Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
```

Anda akan menerima output berikut.

```
DomainJoinDns : OldIP1,OldIP2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon\SkyLight
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon
PSChildName   : SkyLight
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
```

4. Di PowerShell jendela, jalankan perintah berikut untuk mengubah *OldIP1* ke*NewIP1*. Pastikan untuk meninggalkan *OldIP2* seperti saat ini.

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
 "NewIP1,OldIP2"
```

5. Jalankan perintah berikut untuk memulai ulang layanan SkyLightWorkspaceConfigService.

```
restart-service -Name SkyLightWorkspaceConfigService
```

> **Note**
>
> Setelah Anda me-restart layanan SkyLightWorkspaceConfigService, dapat memakan waktu hingga 1 menit untuk adaptor jaringan untuk mencerminkan perubahan.

6. Lanjutkan ke Langkah 2, dan perbarui pengaturan server DNS Anda di Direktori Aktif untuk menggantikan *OldIP1* dengan *NewIP1*.

Perbarui pengaturan server DNS untuk Linux WorkSpaces

Jika Anda memiliki lebih dari satu Linux WorkSpace, kami sarankan Anda menggunakan solusi manajemen konfigurasi untuk mendistribusikan dan menegakkan kebijakan. Misalnya, Anda dapat menggunakan AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise, atau Ansible.

Untuk memperbarui pengaturan server DNS di Linux WorkSpace

1. Di Linux Anda WorkSpace, buka jendela Terminal (Applications > System Tools > MATE Terminal).
2. Gunakan perintah Linux berikut untuk mengedit file `/etc/dhcp/dhclient.conf`. Anda harus memiliki hak pengguna root untuk mengedit file ini. Entah menjadi root dengan menggunakan `sudo -i` perintah, atau menjalankan semua perintah dengan `sudo` seperti yang ditunjukkan.

   ```
   sudo vi /etc/dhcp/dhclient.conf
   ```

   Di file `/etc/dhcp/dhclient.conf`, Anda akan melihat perintah `prepend` berikut, saat *`OldIP1`* dan *`OldIP2`* merupakan alamat IP dari server DNS Anda.

   ```
   prepend domain-name-servers OldIP1, OldIP2; # skylight
   ```
3. Ganti *`OldIP1`* dengan *`NewIP1`*, dan biarkan *`OldIP2`* apa adanya untuk saat ini.
4. Simpan perubahan Anda ke `/etc/dhcp/dhclient.conf`.
5. Nyalakan ulang WorkSpace.
6. Lanjutkan ke Langkah 2, dan perbarui pengaturan server DNS Anda di Direktori Aktif untuk menggantikan *`OldIP1`* dengan *`NewIP1`*.

Langkah 2: Perbarui pengaturan server DNS untuk Direktori Aktif

Pada langkah ini, Anda memperbarui pengaturan server DNS untuk Direktori Aktif. Sebagaimana dicatat dalam bagian Praktik Terbaik, kami merekomendasikan memperbarui alamat IP server DNS Anda satu per satu.

Untuk memperbarui pengaturan server DNS untuk Direktori Aktif, lihat dokumentasi berikut di Panduan Administrasi AWS Directory Service:

- AD Connector: Perbarui alamat DNS untuk AD Connector Anda
- Microsoft AD yang Dikelola AWS: Konfigurasikan Forwarders bersyarat DNS untuk Domain On-premise Anda
- Simple AD: Konfigurasi DNS

Setelah memperbarui pengaturan server DNS, lanjutkan ke Langkah 3.

Langkah 3: Uji pengaturan server DNS yang diperbarui

Setelah menyelesaikan Langkah 1 dan Langkah 2, gunakan prosedur berikut untuk memverifikasi bahwa pengaturan server DNS yang diperbarui berfungsi seperti yang diharapkan.

Dalam prosedur berikut, nilai alamat IP server DNS saat ini dan yang baru disebut sebagai berikut:

- Alamat IP DNS saat ini: *OldIP1*, *OldIP2*
- Alamat IP DNS baru: *NewIP1*, *NewIP2*

> **Note**
>
> Jika ini adalah kedua kalinya Anda melakukan prosedur ini, ganti *OldIP1* dengan *OldIP2* dan *NewIP1* dengan *NewIP2*.

Uji pengaturan server DNS yang diperbarui untuk Windows WorkSpaces

1. Matikan server DNS *OldIP1*.
2. Masuk ke Windows WorkSpace.
3. Pada menu Mulai Windows, pilih Windows System, lalu pilih Command Prompt.
4. Jalankan perintah berikut, saat *AD_Name* adalah nama Direktori Aktif (misalnya, `corp.example.com`).

   ```
   nslookup AD_Name
   ```

   Perintah `nslookup` harus mengembalikan output berikut. (Jika ini adalah kedua kalinya Anda melakukan prosedur ini, Anda akan melihat *NewIP2* di tempat *OldIP2*.)

   ```
   Server:  Full_AD_Name
   Address:  NewIP1

   Name:    AD_Name
   Addresses:  OldIP2
             NewIP1
   ```

5. Jika output tidak seperti yang Anda harapkan atau jika Anda menerima kesalahan, ulangi Langkah 1.

6. Tunggu selama satu jam dan konfirmasikan bahwa tidak ada masalah pengguna yang dilaporkan. Verifikasi bahwa *NewIP1* mendapatkan kueri DNS dan merespons dengan jawaban.
7. Setelah Anda memverifikasi bahwa server DNS pertama berfungsi dengan baik, ulangi Langkah 1 untuk memperbarui server DNS kedua, kali ini ganti *OldIP2* dengan *NewIP2*. Kemudian ulangi Langkah 2 dan Langkah 3.

Uji pengaturan server DNS yang diperbarui untuk Linux WorkSpaces

1. Matikan server DNS *OldIP1*.
2. Masuk ke Linux WorkSpace.
3. Di Linux Anda WorkSpace, buka jendela Terminal (Applications > System Tools > MATE Terminal).
4. Alamat IP server DNS yang dikembalikan dalam respons DHCP ditulis ke `/etc/resolv.conf` file lokal di file. WorkSpace Jalankan perintah berikut untuk menampilkan isi file `/etc/resolv.conf` .

   ```
   cat /etc/resolv.conf
   ```

   Anda akan melihat output berikut. (Jika ini adalah kedua kalinya Anda melakukan prosedur ini, Anda akan melihat *NewIP2* di tempat *OldIP2*.)

   ```
   ; This file is generated by Amazon WorkSpaces
   ; Modifying it can make your WorkSpace inaccessible until reboot
   options timeout:2 attempts:5
   ; generated by /usr/sbin/dhclient-script
   search region.compute.internal
   nameserver NewIP1
   nameserver OldIP2
   nameserver WorkSpaceIP
   ```

   > **Note**
   >
   > Jika Anda membuat modifikasi manual pada `/etc/resolv.conf` file, perubahan tersebut hilang saat dimulai ulang. WorkSpace

5. Jika output tidak seperti yang Anda harapkan atau jika Anda menerima kesalahan, ulangi Langkah 1.

6. Alamat IP server DNS yang sebenarnya disimpan dalam file `/etc/dhcp/dhclient.conf`. Untuk melihat isi file ini, jalankan perintah berikut.

   ```
   sudo cat /etc/dhcp/dhclient.conf
   ```

   Anda akan melihat output berikut. (Jika ini adalah kedua kalinya Anda melakukan prosedur ini, Anda akan melihat *NewIP2* di tempat *OldIP2*.)

   ```
   # This file is generated by Amazon WorkSpaces
   # Modifying it can make your WorkSpace inaccessible until rebuild
   prepend domain-name-servers NewIP1, OldIP2; # skylight
   ```

7. Tunggu selama satu jam dan konfirmasi bahwa tidak ada masalah pengguna yang dilaporkan. Verifikasi bahwa *NewIP1* mendapatkan kueri DNS dan merespons dengan jawaban.
8. Setelah Anda memverifikasi bahwa server DNS pertama berfungsi dengan baik, ulangi Langkah 1 untuk memperbarui server DNS kedua, kali ini ganti *OldIP2* dengan *NewIP2*. Kemudian ulangi Langkah 2 dan Langkah 3.

Hapus direktori untuk WorkSpaces

Anda dapat menghapus direktori untuk Anda WorkSpaces jika tidak lagi digunakan oleh aplikasi lain WorkSpaces atau lainnya, seperti Amazon, Amazon WorkDocs WorkMail, atau Amazon Chime. Perhatikan bahwa Anda harus membatalkan pendaftaran direktori sebelum dapat menghapusnya.

> **Note**
>
> Simple AD dan AD Connector tersedia untuk Anda secara gratis untuk digunakan WorkSpaces. Jika tidak ada yang WorkSpaces digunakan dengan direktori Simple AD atau AD Connector selama 30 hari berturut-turut, direktori ini akan secara otomatis dideregistrasi untuk digunakan dengan Amazon WorkSpaces, dan Anda akan dikenakan biaya untuk direktori ini sesuai ketentuan harga. AWS Directory Service
> Jika Anda menghapus direktori Simple AD atau AD Connector, Anda selalu dapat membuat yang baru ketika Anda ingin mulai menggunakan WorkSpaces lagi.

Hal yang akan terjadi jika Anda menghapus sebuah direktori

Ketika Simple AD atau direktori AWS Directory Service for Microsoft Active Directory dihapus, semua data direktori dan snapshot dihapus dan tidak dapat dipulihkan. Setelah direktori dihapus, semua instans Amazon EC2 yang bergabung ke direktori tetap utuh. Namun, Anda tidak dapat menggunakan kredensial direktori Anda untuk log in ke instans ini. Anda harus masuk ke instance ini dengan Akun AWS yang lokal untuk instance.

Ketika direktori AD Connector dihapus, direktori on-premise Anda tetap utuh. Semua instans Amazon EC2 yang digabungkan ke direktori juga tetap utuh dan tetap bergabung dengan direktori on-premise Anda. Anda masih bisa menggunakan kredensial direktori Anda untuk log in ke instans ini.

Untuk menghapus direktori

1. Hapus semua WorkSpaces di direktori. Untuk informasi selengkapnya, lihat Menghapus WorkSpace.
2. Temukan dan hapus semua aplikasi dan layanan yang terdaftar ke direktori. Untuk informasi selengkapnya, lihat Hapus Direktori Anda dalam Panduan Administrasi AWS Directory Service.
3. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
4. Di panel navigasi, pilih Direktori.
5. Pilih direktori dan pilih Tindakan, Batalkan Pendaftaran.
6. Ketika diminta konfirmasi, pilih Batalkan Pendaftaran.
7. Pilih direktori kembali dan pilih Tindakan, Hapus.
8. Saat diminta konfirmasi, pilih Delete (Hapus).

> **Note**
>
> Menghapus tugas aplikasi terkadang membutuhkan lebih banyak waktu dari yang diduga. Jika Anda menerima pesan kesalahan berikut, verifikasi bahwa Anda telah menghapus semua tugas aplikasi, lalu tunggu selama 30 hingga 60 menit sebelum mencoba kembali untuk menghapus direktori:
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (Opsional) Setelah Anda menghapus semua sumber daya di virtual private cloud (VPC) untuk direktori Anda, Anda dapat menghapus VPC dan merilis Alamat IP elastis yang digunakan untuk

NAT gateway. Untuk informasi selengkapnya, lihat Menghapus VPC Anda dan Bekerja dengan alamat IP Elastis dalam Panduan Pengguna Amazon VPC.

10. (Opsional) Untuk menghapus semua paket kustom dan citra yang telah Anda selesaikan, lihat Hapus WorkSpaces bundel atau gambar khusus.

Aktifkan Amazon WorkDocs untuk Microsoft AD yang AWS Dikelola

Jika Anda menggunakan Microsoft AD yang AWS Dikelola dengan Amazon WorkSpaces, Anda dapat mengaktifkan Amazon WorkDocs untuk direktori Anda melalui WorkDocs konsol Amazon atau AWS Directory Service konsol.

> **Note**
>
> Amazon WorkDocs tidak tersedia di semua AWS Wilayah tempat Amazon WorkSpaces tersedia. Untuk informasi selengkapnya, lihat WorkDocs Harga Amazon.

Untuk mengaktifkan WorkDocs melalui WorkDocs konsol Amazon

1. Buka WorkDocs konsol Amazon di https://console.aws.amazon.com/zocalo/.
2. Pilih Buat WorkDocs Situs Baru.
3. Di bawah Penyiapan Standar, pilih Luncurkan.
4. Pilih direktori dan buat nama situs Anda.
5. Tentukan pengguna yang akan mengelola WorkDocs situs. Anda dapat menggunakan admin atau pengguna yang dibuat dalam direktori.

Untuk informasi selengkapnya, lihat Memulai dengan Microsoft AD yang AWS Dikelola di Panduan WorkDocs Administrasi Amazon.

Untuk mengaktifkan WorkDocs melalui AWS Directory Service konsol

1. Buka konsol AWS Directory Service di https://console.aws.amazon.com/directoryservicev2/.
2. Di panel navigasi, pilih Direktori.
3. Di halaman Direktori, pilih direktori Anda.
4. Di halaman Detail direktori, pilih tab Pengelolaan aplikasi.

5. Di bagian URL akses aplikasi, jika URL akses belum ditetapkan ke direktori, tombol Buat ditampilkan. Masukkan alias direktori dan pilih Buat. Untuk informasi selengkapnya, lihat Membuat URL Akses dalam Panduan Administrasi AWS Directory Service.
6. Di bagian URL akses aplikasi, pilih Aktifkan untuk mengaktifkan sistem masuk tunggal untuk Amazon. WorkDocs Untuk informasi selengkapnya, lihat Sign-On Tunggal dalam Panduan Administrasi AWS Directory Service.

Siapkan Alat Administrasi Direktori Aktif untuk WorkSpaces

Anda akan melakukan sebagian besar tugas administratif untuk WorkSpaces direktori Anda menggunakan alat manajemen direktori, seperti Alat Administrasi Direktori Aktif. Namun, Anda akan menggunakan WorkSpaces konsol untuk melakukan beberapa tugas terkait direktori. Untuk informasi selengkapnya, lihat Kelola direktori untuk WorkSpaces.

Jika Anda membuat direktori dengan Microsoft AD AWS Terkelola atau Simple AD yang menyertakan lima atau lebih WorkSpaces, sebaiknya Anda memusatkan administrasi pada instans Amazon EC2. Meskipun Anda dapat menginstal alat manajemen direktori pada WorkSpace, menggunakan instans Amazon EC2 adalah solusi yang lebih kuat.

Untuk menyiapkan Alat Administrasi Direktori Aktif

1. Luncurkan instans Windows Amazon EC2 dan gabungkan ke WorkSpaces direktori Anda dengan menggunakan salah satu opsi berikut:
   - Jika Anda tidak sudah memiliki instans Windows Amazon EC2 yang ada, Anda dapat bergabung dengan instans untuk domain direktori Anda ketika Anda meluncurkan instans. Untuk informasi lebih lanjut, lihat Bergabung dengan Instans Windows EC2 di Panduan Administrasi AWS Directory Service.
   - Jika Anda sudah memiliki instans Windows Amazon EC2 yang ada, Anda dapat bergabung ke direktori Anda secara manual. Untuk informasi selengkapnya, lihat Menambahkan instans Windows secara manual di Panduan Administrasi AWS Directory Service.
2. Instal Alat Administrasi Direktori Aktif pada instans Windows Amazon EC2. Untuk informasi selengkapnya, lihat Menginstal alat administrasi direktori aktif di Panduan Administrasi AWS Directory Service.

> **Note**
>
> Ketika Anda menginstal Alat Administrasi Direktori Aktif, pastikan untuk juga memilih Manajemen Kebijakan Grup untuk menginstal alat (gpmc.msc) Editor Manajemen Kebijakan Grup.

Setelah penginstalan fitur selesai, alat Direktori Aktif tersedia di menu mulai Windows di Alat Administratif Windows.

3. Jalankan alat sebagai administrator direktori sebagai berikut:

   a. Pada menu mulai Windows, bukaAlat Administratif Windows.

   b. Tekan terus tombol Shift, klik kanan pintasan alat yang ingin Anda gunakan, lalu pilih Jalankan sebagai pengguna yang berbeda.

   c. Masukkan kredensi masuk untuk administrator. Dengan Simple AD, nama penggunanya adalah **`Administrator`** dan dengan Microsoft AD Terkelola AWS, administratornya adalah **`Admin`**.

Anda sekarang dapat melakukan tugas administrasi direktori menggunakan alat Direktori Aktif yang Anda kenal. Misalnya, Anda dapat menggunakan Pengguna dan Alat Komputer Direktori Aktif untuk menambahkan pengguna, menghapus pengguna, mempromosikan pengguna ke administrator direktori, atau mengatur ulang kata sandi pengguna. Perhatikan bahwa Anda harus login ke instans Windows Anda sebagai pengguna yang memiliki izin untuk mengelola pengguna dalam direktori.

Untuk mempromosikan pengguna ke administrator direktori

> **Note**
>
> Prosedur ini hanya berlaku untuk direktori yang dibuat dengan Simple AD, bukan AD terkelola AWS. Untuk direktori yang dibuat dengan AD terkelola AWS, lihat Kelola Pengguna dan Grup di Microsoft AD Terkelola AWS di Panduan Administrasi AWS Directory Service.

1. Buka alat Pengguna dan Komputer Direktori Aktif.
2. Arahkan ke folder Pengguna di bawah domain Anda dan pilih pengguna yang akan dipromosikan.

3. Pilih Tindakan, Properti.
4. Di kotak dialog properti ***nama pengguna***, pilih Anggota Dari.
5. Tambahkan pengguna ke grup berikut dan pilih OKE.
   - Administrator
   - Domain Admin
   - Admin Perusahaan
   - Pemilik Pembuat Kebijakan Grup
   - Skema Admin

Untuk menambahkan atau menghapus pengguna

Anda dapat membuat pengguna baru dari WorkSpaces konsol Amazon hanya selama proses peluncuran WorkSpace, dan Anda tidak dapat menghapus pengguna melalui WorkSpaces konsol Amazon. Sebagian besar tugas manajemen pengguna, termasuk mengelola grup pengguna, harus dilakukan melalui direktori Anda.

> **Important**
>
> Sebelum Anda dapat menghapus pengguna, Anda harus menghapus yang WorkSpace ditetapkan untuk pengguna itu. Untuk informasi selengkapnya, lihat Menghapus WorkSpace.

Proses yang Anda gunakan untuk mengelola pengguna dan grup tergantung pada tipe direktori yang Anda gunakan.

- Jika Anda menggunakan Microsoft AD terkelola AWS, lihat Kelola Pengguna dan Grup di Microsoft AD terkelola AWS di Panduan Administrasi AWS Directory Service.
- Jika Anda menggunakan Simple AD, lihat Kelola Pengguna dan Grup di Simple AD di Panduan Administrasi AWS Directory Service.
- Jika Anda menggunakan Microsoft Active Directory melalui AD Connector atau hubungan kepercayaan, Anda dapat mengelola pengguna dan grup menggunakan modul Active Directory.

Cara mengatur ulang kata sandi pengguna

Saat Anda mengatur ulang kata sandi untuk pengguna yang ada, jangan tetapkan Pengguna harus mengubah sandi pada logon berikutnya. Jika tidak, pengguna tidak dapat terhubung ke mereka WorkSpaces. Sebagai gantinya, tetapkan kata sandi sementara yang aman untuk setiap pengguna dan kemudian minta pengguna untuk mengubah kata sandi mereka secara manual dari dalam waktu berikutnya mereka masuk. WorkSpace

> **Note**
>
> Jika Anda menggunakan AD Connector atau jika pengguna Anda berada di Wilayah AWS GovCloud (AS-Barat), pengguna Anda tidak akan dapat mengatur ulang kata sandi mereka sendiri. (Lupa kata sandi? pilihan pada layar login aplikasi WorkSpaces klien tidak akan tersedia.)

Luncurkan desktop virtual menggunakan WorkSpaces

Dengan WorkSpaces, Anda dapat menyediakan desktop Microsoft Windows, Amazon Linux, atau Ubuntu Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai. WorkSpaces

> **Note**
>
> Nilai Nama Komputer yang WorkSpace ditampilkan untuk WorkSpaces konsol Amazon bervariasi, tergantung pada jenis yang WorkSpace Anda luncurkan (Amazon Linux, Ubuntu, atau Windows). Nama komputer untuk a WorkSpace dapat dalam salah satu format ini:
>
> - Amazon Linux: A- *xxxxxxxxxxxxx*
> - Ubuntu: U- *xxxxxxxxxxxxx*
> - Windows: IP-C*xxxxxx* atau WSAMZN-*xxxxxxx* atau EC2AMAZ-*xxxxxxx*
>
> Untuk Windows WorkSpaces, format nama komputer ditentukan oleh jenis bundel, dan dalam kasus WorkSpaces dibuat dari bundel publik atau dari bundel khusus berdasarkan gambar publik, ketika gambar publik dibuat.
> *Mulai 22 Juni 2020, Windows yang WorkSpaces diluncurkan dari bundel publik memiliki format WSAMZN- xxxxxxx untuk nama komputer mereka alih-alih format IP-C xxxxxx.*
> Untuk paket kustom berdasarkan citra publik, jika citra publik dibuat sebelum 22 Juni 2020, nama komputer dalam format EC2AMAZ-*xxxxxxx*. Jika citra publik dibuat pada atau setelah 22 Juni 2020, nama komputer berada dalam format WSAMZN-*xxxxxxx*.
> Untuk paket Bawa Lisensi Anda Sendiri (BYOL), format DESKTOP-*xxxxxxx* atau EC2AMAZ-*xxxxxxx* digunakan untuk nama komputer secara default.
> Jika Anda telah menentukan format kustom untuk nama komputer dalam paket kustom atau BYOL, format kustom Anda akan menggantikan format default ini. Untuk menentukan format kustom, lihat Buat WorkSpaces gambar dan bundel khusus.
> Penting — Jika Anda mengubah nama komputer untuk WorkSpace melalui pengaturan sistem Windows, Anda tidak akan lagi dapat mengakses WorkSpace.

WorkSpaces menggunakan direktori untuk menyimpan dan mengelola informasi untuk Anda WorkSpaces dan pengguna. Lakukan langkah-langkah berikut:

- Buat direktori Simple AD.
- Buat AWS Directory Service untuk Direktori Aktif Microsoft, juga dikenal sebagai Microsoft AD yang dikelola AWS.
- Hubungkan ke Direktori Aktif Microsoft yang ada dengan menggunakan Konektor Direktori Aktif.
- Buat hubungan kepercayaan antara direktori Microsoft AD yang Dikelola AWS dan domain on-premise Anda.

> **Note**
>
> - Direktori bersama saat ini tidak didukung untuk digunakan dengan Amazon WorkSpaces.
> - Jika Anda mengonfigurasi direktori Microsoft AD AWS Terkelola untuk replikasi Multi-wilayah, hanya direktori di Wilayah utama yang dapat didaftarkan untuk digunakan dengan Amazon. WorkSpaces Upaya untuk mendaftarkan direktori di Wilayah yang direplikasi untuk digunakan dengan Amazon WorkSpaces akan gagal. Replikasi Multi-Wilayah dengan AWS Microsoft AD Terkelola tidak didukung untuk digunakan dengan Amazon WorkSpaces dalam Wilayah yang direplikasi.
> - Simple AD dan AD Connector tersedia untuk Anda secara gratis untuk digunakan WorkSpaces. Jika tidak ada yang WorkSpaces digunakan dengan direktori Simple AD atau AD Connector selama 30 hari berturut-turut, direktori ini akan secara otomatis dideregistrasi untuk digunakan dengan Amazon WorkSpaces, dan Anda akan dikenakan biaya untuk direktori ini sesuai ketentuan harga. AWS Directory Service
>
>   Untuk menghapus direktori kosong, lihat Hapus direktori untuk WorkSpaces. Jika Anda menghapus direktori Simple AD atau AD Connector, Anda selalu dapat membuat yang baru ketika Anda ingin mulai menggunakan WorkSpaces lagi.

Tutorial berikut menunjukkan cara meluncurkan WorkSpace dengan menggunakan opsi layanan direktori yang didukung.

Tutorial

- Luncurkan WorkSpace menggunakan Microsoft AD yang AWS Dikelola
- Luncurkan WorkSpace menggunakan Simple AD
- Luncurkan WorkSpace menggunakan AD Connector
- Luncurkan WorkSpace menggunakan domain tepercaya

Luncurkan WorkSpace menggunakan Microsoft AD yang AWS Dikelola

WorkSpaces memungkinkan Anda menyediakan desktop Windows dan Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai. WorkSpaces

WorkSpaces menggunakan direktori untuk menyimpan dan mengelola informasi untuk Anda WorkSpaces dan pengguna. Untuk direktori Anda, Anda dapat memilih dari Simple AD, AD Connector, atau AWS Directory Service untuk Direktori Aktif, juga dikenal sebagai Microsoft AD Terkelola AWS. Selain itu, Anda dapat membangun hubungan kepercayaan antara direktori AWS Managed Microsoft AD dan domain on-premise Anda.

Dalam tutorial ini, kami meluncurkan WorkSpace yang menggunakan AWS Managed Microsoft AD. Untuk tutorial yang menggunakan opsi lainnya, lihat Luncurkan desktop virtual menggunakan WorkSpaces.

Tugas

Sebelum Anda memulai

- WorkSpaces tidak tersedia di setiap wilayah. Verifikasi Wilayah yang didukung dan pilih Wilayah untuk Anda WorkSpaces. Untuk informasi selengkapnya tentang Wilayah yang didukung, lihat WorkSpaces Harga menurut AWS Wilayah.
- Saat Anda meluncurkan WorkSpace, Anda harus memilih WorkSpace bundel. Sebuah paket adalah kombinasi dari sistem pengoperasian, dan penyimpanan, komputasi, dan sumber daya perangkat lunak. Untuk informasi selengkapnya, lihat Amazon WorkSpaces Bundles.
- Saat Anda membuat direktori menggunakan AWS Directory Service atau meluncurkan WorkSpace, Anda harus membuat atau memilih cloud pribadi virtual yang dikonfigurasi dengan subnet publik dan dua subnet pribadi. Untuk informasi selengkapnya, lihat Konfigurasikan VPC untuk WorkSpaces.

Langkah 1: Buat Direktori AWS Managed Microsoft AD

Pertama, buat direktori AWS Managed Microsoft AD. AWS Directory Service membuat dua server direktori, satu di setiap subnet privat VPC Anda. Perhatikan bahwa awalnya tidak ada pengguna di direktori. Anda akan menambahkan pengguna di langkah berikutnya ketika Anda meluncurkan WorkSpace.

> **Note**
>
> - Direktori bersama saat ini tidak didukung untuk digunakan dengan Amazon WorkSpaces.
> - Jika direktori Microsoft AD AWS Terkelola Anda telah dikonfigurasi untuk replikasi Multi-wilayah, hanya direktori di Wilayah utama yang dapat didaftarkan untuk digunakan dengan Amazon. WorkSpaces Upaya untuk mendaftarkan direktori di Wilayah yang direplikasi untuk digunakan dengan Amazon WorkSpaces akan gagal. Replikasi Multi-Wilayah dengan AWS Microsoft AD Terkelola tidak didukung untuk digunakan dengan Amazon WorkSpaces dalam Wilayah yang direplikasi.

Untuk membuat direktori AWS Managed Microsoft AD

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih Siapkan Direktori, Buat Microsoft AD.
4. Konfigurasikan direktori sebagai berikut:

    a. Untuk nama Organisasi, masukkan nama organisasi unik untuk direktori Anda (misalnya, my-demo-directory). Nama ini harus terdiri dari setidaknya empat karakter, hanya terdiri dari karakter alfanumerik dan tanda hubung (-), dan dimulai atau diakhiri dengan karakter selain tanda hubung.

    b. Untuk DNS direktori, masukkan nama direktori yang memenuhi syarat (misalnya, workspaces.demo.com).

> **Important**
>
> Jika Anda perlu memperbarui server DNS Anda setelah meluncurkan Anda WorkSpaces, ikuti prosedur Perbarui server DNS untuk Amazon WorkSpaces untuk memastikan bahwa WorkSpaces Anda diperbarui dengan benar.

c. Untuk Nama NetBIOS, masukkan nama singkat untuk direktori (misalnya, workspaces).

d. Untuk Kata sandi admin dan Konfirmasi kata sandi, masukkan kata sandi untuk akun administrator direktori. Untuk informasi selengkapnya tentang persyaratan kata sandi, lihat Buat Direktori AWS Managed Microsoft AD Anda dalam Panduan Administrasi AWS Directory Service.

e. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk direktori.

f. Untuk VPC, pilih VPC yang Anda buat.

g. Untuk Subnet, pilih dua subnet privat (dengan blok CIDR `10.0.1.0/24` dan `10.0.2.0/24`).

h. Pilih Langkah Selanjutnya.

5. Pilih Buat Microsoft AD.
6. Pilih Selesai. Status awal dari direktori adalah `Creating`. Ketika pembuatan direktori selesai, statusnya adalah `Active`.

Langkah 2: Buat WorkSpace

Sekarang Anda telah membuat direktori Microsoft AD yang AWS Dikelola, Anda siap untuk membuat direktori WorkSpace.

Untuk membuat WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih Luncurkan WorkSpaces.
4. Pada halaman Pilih Direktori, pilih direktori yang Anda buat, lalu pilih Langkah Berikutnya. WorkSpacesmendaftarkan direktori Anda.
5. Pada halaman Identifikasi Pengguna, tambahkan pengguna baru ke direktori Anda sebagai berikut:

a. Lengkapi Nama pengguna, Nama Pertama, Nama Terakhir, dan Email. Gunakan alamat email yang dapat Anda akses.

b. Pilih Buat Pengguna.

c. Pilih Langkah Selanjutnya.

6. Pada halaman Pilih Paket, pilih paket lalu pilih Langkah Selanjutnya.

> **Note**
>
> Tinjau penggunaan dan spesifikasi yang disarankan dari setiap bundel untuk membantu memastikan Anda memilih bundel yang paling sesuai untuk pengguna Anda. Untuk informasi selengkapnya tentang setiap kasus penggunaan, lihat Amazon WorkSpaces Bundles. Untuk informasi selengkapnya tentang spesifikasi bundel, penggunaan yang disarankan, dan harga, lihat WorkSpaces harga Amazon.

7. Pada halaman WorkSpaces Konfigurasi, pilih mode berjalan dan kemudian pilih Langkah Berikutnya.

8. Pada WorkSpaces halaman Review & Launch, pilih Launch WorkSpaces. Status awal WorkSpace adalah`PENDING`. Saat peluncuran selesai, statusnya adalah `AVAILABLE` dan undangan dikirim ke alamat email yang Anda tentukan untuk pengguna.

> **Note**
>
> Email undangan tidak dikirim jika pengguna sudah ada di Direktori Aktif. Sebagai gantinya, pastikan Anda mengirim email undangan secara manual kepada pengguna. Untuk informasi selengkapnya, lihat Kirim email undangan.

9. (Opsional) Jika Amazon WorkDocs didukung di Wilayah, Anda dapat mengaktifkan Amazon WorkDocs untuk semua pengguna di direktori. Untuk informasi selengkapnya, lihat Aktifkan Amazon WorkDocs untuk Microsoft AD yang AWS Dikelola. Untuk informasi selengkapnya tentang Amazon WorkDocs, lihat Amazon WorkDocs Drive di Panduan WorkDocs Administrasi Amazon.

Langkah 3: Connect ke WorkSpace

Setelah Anda menerima email undangan, Anda dapat terhubung ke Anda WorkSpace menggunakan klien pilihan Anda. Setelah Anda masuk, klien akan menampilkan WorkSpace desktop.

Untuk terhubung ke WorkSpace

1. Buka tautan di email undangan. Saat diminta, tentukan kata sandi dan aktifkan pengguna. Ingat kata sandi ini karena Anda akan memerlukannya untuk masuk ke Anda WorkSpace.

   > **Note**
   >
   > Kata sandi peka terhadap huruf kapabilitas dan harus terdiri dari 8 hingga 64 karakter. Kata sandi harus berisi setidaknya satu karakter dari masing-masing kategori berikut: huruf kecil (a-z), huruf besar (A-Z), angka (0-9), dan ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Tinjau WorkSpaces Klien di Panduan WorkSpaces Pengguna Amazon untuk informasi selengkapnya tentang persyaratan untuk setiap klien, lalu lakukan salah satu hal berikut:

   - Saat diminta, unduh salah satu aplikasi client atau luncurkan Akses Web.
   - Jika Anda tidak diminta dan Anda belum menginstal aplikasi klien, buka https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

   > **Note**
   >
   > Anda tidak dapat menggunakan browser web (Akses Web) untuk terhubung ke Amazon Linux WorkSpaces.

3. Mulai client, masukkan kode pendaftaran dari email undangan, dan pilih Daftar.
4. Saat diminta untuk masuk, masukkan kredenal masuk pengguna, lalu pilih Masuk.
5. (Opsional) Saat diminta untuk menyimpan kredensial, pilih Ya.

Langkah selanjutnya

Anda dapat terus menyesuaikan WorkSpace yang baru saja Anda buat. Misalnya, Anda dapat menginstal perangkat lunak dan kemudian membuat bundel khusus dari Anda WorkSpace. Anda juga dapat melakukan berbagai tugas administratif untuk WorkSpaces direktori Anda WorkSpaces dan Anda. Jika Anda selesai dengan Anda WorkSpace, Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat dokumentasi berikut.

- Buat WorkSpaces gambar dan bundel khusus
- Kelola Anda WorkSpaces

- Kelola direktori untuk WorkSpaces
- Menghapus WorkSpace

Untuk informasi selengkapnya tentang penggunaan aplikasi WorkSpaces klien, seperti menyiapkan beberapa monitor atau menggunakan perangkat periferal, lihat Dukungan WorkSpaces Klien dan Perangkat Periferal di Panduan WorkSpaces Pengguna Amazon.

Luncurkan WorkSpace menggunakan Simple AD

WorkSpaces memungkinkan Anda menyediakan desktop Microsoft Windows dan Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai. WorkSpaces

WorkSpaces menggunakan direktori untuk menyimpan dan mengelola informasi untuk Anda WorkSpaces dan pengguna. Untuk direktori Anda, Anda dapat memilih dari Simple AD, AD Connector, atau AWS Directory Service untuk Direktori Aktif, juga dikenal sebagai Microsoft AD Terkelola AWS. Selain itu, Anda dapat membangun hubungan kepercayaan antara direktori AWS Managed Microsoft AD dan domain on-premise Anda.

Dalam tutorial ini, kami meluncurkan WorkSpace yang menggunakan Simple AD. Untuk tutorial yang menggunakan opsi lainnya, lihat Luncurkan desktop virtual menggunakan WorkSpaces.

Tugas

- Sebelum Anda memulai
- Langkah 1: Buat direktori Simple AD
- Langkah 2: Buat WorkSpace
- Langkah 3: Connect ke WorkSpace
- Langkah selanjutnya

Sebelum Anda memulai

- Simple AD tidak tersedia di setiap Wilayah. Verifikasi Wilayah yang didukung dan pilih sebuah Wilayahuntuk direktori Simple AD Anda. Untuk informasi selengkapnya tentang Wilayah yang didukung untuk Simple AD, lihat Ketersediaan Wilayah untuk AWS Directory Service .
- WorkSpaces tidak tersedia di setiap wilayah. Verifikasi Wilayah yang didukung dan pilih Wilayah untuk Anda WorkSpaces. Untuk informasi selengkapnya tentang Wilayah yang didukung, lihat WorkSpaces Harga menurut AWS Wilayah.

- Saat Anda meluncurkan WorkSpace, Anda harus memilih WorkSpace bundel. Sebuah paket adalah kombinasi dari sistem pengoperasian, dan penyimpanan, komputasi, dan sumber daya perangkat lunak. Untuk informasi selengkapnya, lihat Amazon WorkSpaces Bundles.
- Saat Anda membuat direktori menggunakan AWS Directory Service atau meluncurkan WorkSpace, Anda harus membuat atau memilih cloud pribadi virtual yang dikonfigurasi dengan subnet publik dan dua subnet pribadi. Untuk informasi selengkapnya, lihat Konfigurasikan VPC untuk WorkSpaces.

Langkah 1: Buat direktori Simple AD

Membuat direktori Simple AD. AWS Directory Service membuat dua server direktori, satu di setiap subnet privat VPC Anda. Perhatikan bahwa awalnya tidak ada pengguna di direktori. Anda akan menambahkan pengguna di langkah berikutnya saat Anda membuat file WorkSpace.

> **Note**
>
> Simple AD tersedia untuk Anda secara gratis untuk digunakan WorkSpaces. Jika tidak ada yang WorkSpaces digunakan dengan direktori Simple AD Anda selama 30 hari berturut-turut, direktori ini akan secara otomatis dideregistrasi untuk digunakan dengan Amazon WorkSpaces, dan Anda akan dikenakan biaya untuk direktori ini sesuai ketentuan harga. AWS Directory Service
>
> Untuk menghapus direktori kosong, lihat Hapus direktori untuk WorkSpaces. Jika Anda menghapus direktori Simple AD Anda, Anda selalu dapat membuat yang baru ketika Anda ingin mulai menggunakan WorkSpaces lagi.

Untuk membuat direktori Simple AD

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih Siapkan Direktori, Simple AD, dan Selanjutnya.
4. Konfigurasikan direktori sebagai berikut:

    a. Untuk nama Organisasi, masukkan nama organisasi unik untuk direktori Anda (misalnya, my-example-directory). Nama ini harus terdiri dari setidaknya empat karakter, hanya terdiri dari karakter alfanumerik dan tanda hubung (-), dan dimulai atau diakhiri dengan karakter selain tanda hubung.

b. Untuk Nama DNS Direktori, masukkan nama yang sepenuhnya memenuhi syarat untuk direktori (misalnya, example.com).

> **Important**
>
> Jika Anda perlu memperbarui server DNS Anda setelah meluncurkan Anda WorkSpaces, ikuti prosedur Perbarui server DNS untuk Amazon WorkSpaces untuk memastikan bahwa WorkSpaces Anda diperbarui dengan benar.

c. Untuk Nama NetBIOS, masukkan nama singkat untuk direktori (misalnya, example).

d. Untuk Kata sandi admin dan Konfirmasikan kata sandi masukkan kata sandi untuk akun administrator direktori. Untuk informasi selengkapnya tentang persyaratan kata sandi, lihat Cara membuat Direktori Microsoft AD dalam Panduan Administrasi AWS Directory Service.

e. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk direktori tersebut.

f. Untuk Ukuran direktori, pilih Kecil.

g. Untuk VPC, pilih VPC yang Anda buat.

h. Untuk Subnet, pilih dua subnet privat (dengan blok CIDR `10.0.1.0/24` dan `10.0.2.0/24`).

i. Pilih Selanjutnya.

5. Pilih Buat direktori.
6. Status awal direktori adalah `Requested`, lalu `Creating`. Ketika pembuatan direktori selesai (ini mungkin memakan waktu beberapa menit), statusnya adalah `Active`.

Apa yang terjadi selama pembuatan direktori

WorkSpaces menyelesaikan tugas-tugas berikut atas nama Anda:

- Membuat peran IAM untuk memungkinkan WorkSpaces layanan membuat antarmuka jaringan elastis dan daftar direktori Anda WorkSpaces . Peran ini memiliki nama `workspaces_DefaultRole`.
- Menyiapkan direktori Simple AD di VPC yang digunakan untuk menyimpan pengguna dan WorkSpace informasi. Direktori memiliki akun administrator dengan nama pengguna Administrator dan kata sandi yang ditentukan.
- Membuat dua grup keamanan, satu untuk pengontrol direktori dan satu lagi untuk WorkSpaces di direktori.

Langkah 2: Buat WorkSpace

Sekarang Anda siap untuk meluncurkan WorkSpace.

Untuk membuat WorkSpace untuk pengguna

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih Luncurkan WorkSpaces.
4. Di halaman Pilih sebuah Direktori, lakukan hal berikut:
   a. Untuk Direktori, pilih direktori yang Anda buat.
   b. Untuk Aktifkan Izin Layanan Mandiri, pilih Ya atau Tidak dan masukkan deskripsi.
   c. Untuk Aktifkan Amazon WorkDocs, pilih Ya.

      > **Note**
      >
      > Opsi ini hanya tersedia jika Amazon WorkDocs tersedia di Wilayah yang dipilih.

   d. Pilih Langkah Berikutnya. WorkSpaces mendaftarkan direktori Simple AD Anda.
5. Pada halaman Identifikasi Pengguna, tambahkan pengguna baru ke direktori Anda sebagai berikut:
   a. Lengkapi Nama pengguna, Nama Pertama, Nama Terakhir, dan Email. Gunakan alamat email yang dapat Anda akses.
   b. Pilih Buat Pengguna.
   c. Pilih Langkah Selanjutnya.
6. Pada halaman Pilih Paket, pilih paket lalu pilih Langkah Selanjutnya.

> **Note**
>
> Tinjau penggunaan dan spesifikasi yang disarankan dari setiap bundel untuk membantu memastikan Anda memilih bundel yang paling sesuai untuk pengguna Anda. Untuk informasi selengkapnya tentang setiap kasus penggunaan, lihat Amazon WorkSpaces Bundles. Untuk informasi selengkapnya tentang spesifikasi bundel, penggunaan yang disarankan, dan harga, lihat WorkSpaces harga Amazon.

7. Pada halaman WorkSpaces Konfigurasi, pilih mode berjalan dan kemudian pilih Langkah Berikutnya.
8. Pada WorkSpaces halaman Review & Launch, pilih Launch WorkSpaces. Status awal dari WorkSpace adalah`PENDING`. Saat peluncuran selesai (ini bisa memakan waktu hingga 20 menit), statusnya adalah `AVAILABLE` dan undangan dikirim ke alamat email yang Anda tentukan untuk pengguna.

> **Note**
>
> Email undangan tidak dikirim jika pengguna sudah ada di Direktori Aktif. Sebagai gantinya, pastikan Anda mengirim email undangan secara manual kepada pengguna. Untuk informasi selengkapnya, lihat Kirim email undangan.

Langkah 3: Connect ke WorkSpace

Setelah Anda menerima email undangan, Anda dapat terhubung ke Anda WorkSpace menggunakan klien pilihan Anda. Setelah Anda masuk, klien akan menampilkan WorkSpace desktop.

Untuk terhubung ke WorkSpace

1. Buka tautan di email undangan. Saat diminta, masukkan kata sandi dan aktifkan pengguna. Ingat kata sandi ini karena Anda akan memerlukannya untuk masuk ke AndaWorkSpace.

> **Note**
>
> Kata sandi peka terhadap huruf kapabilitas dan harus terdiri dari 8 hingga 64 karakter. Kata sandi harus berisi setidaknya satu karakter dari masing-masing kategori berikut: huruf kecil (a-z), huruf besar (A-Z), angka (0-9), dan ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/.

2. Tinjau WorkSpaces Klien di Panduan WorkSpaces Pengguna Amazon untuk informasi selengkapnya tentang persyaratan untuk setiap klien, lalu lakukan salah satu hal berikut:
   - Saat diminta, unduh salah satu aplikasi client atau luncurkan Akses Web.
   - Jika Anda tidak diminta dan Anda belum menginstal aplikasi klien, buka https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

> **Note**
>
> Anda tidak dapat menggunakan browser web (Akses Web) untuk terhubung ke Amazon Linux WorkSpaces.

3. Mulai client, masukkan kode pendaftaran dari email undangan, dan pilih Daftar.
4. Saat diminta untuk masuk, masukkan kredenal masuk pengguna, lalu pilih Masuk.
5. (Opsional) Saat diminta untuk menyimpan kredensial, pilih Ya.

Langkah selanjutnya

Anda dapat terus menyesuaikan WorkSpace yang baru saja Anda buat. Misalnya, Anda dapat menginstal perangkat lunak dan kemudian membuat bundel khusus dari Anda WorkSpace. Anda juga dapat melakukan berbagai tugas administratif untuk WorkSpaces direktori Anda WorkSpaces dan Anda. Jika Anda selesai dengan Anda WorkSpace, Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat dokumentasi berikut.

- Buat WorkSpaces gambar dan bundel khusus
- Kelola Anda WorkSpaces
- Kelola direktori untuk WorkSpaces
- Menghapus WorkSpace

Untuk informasi selengkapnya tentang penggunaan aplikasi WorkSpaces klien, seperti menyiapkan beberapa monitor atau menggunakan perangkat periferal, lihat Dukungan WorkSpaces Klien dan Perangkat Periferal di Panduan WorkSpaces Pengguna Amazon.

Luncurkan WorkSpace menggunakan AD Connector

WorkSpaces memungkinkan Anda menyediakan desktop Microsoft Windows dan Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai. WorkSpaces

WorkSpaces menggunakan direktori untuk menyimpan dan mengelola informasi untuk Anda WorkSpaces dan pengguna. Untuk direktori Anda, Anda dapat memilih dari Simple AD, AD Connector, atau AWS Directory Service untuk Direktori Aktif, juga dikenal sebagai Microsoft AD

Terkelola AWS. Selain itu, Anda dapat membangun hubungan kepercayaan antara direktori AWS Managed Microsoft AD dan domain on-premise Anda.

Dalam tutorial ini, kami meluncurkan WorkSpace yang menggunakan AD Connector. Untuk tutorial yang menggunakan opsi lainnya, lihat Luncurkan desktop virtual menggunakan WorkSpaces.

Tugas

Sebelum Anda memulai

- WorkSpaces tidak tersedia di setiap wilayah. Verifikasi Wilayah yang didukung dan pilih Wilayah untuk Anda WorkSpaces. Untuk informasi selengkapnya tentang Wilayah yang didukung, lihat WorkSpaces Harga menurut AWS Wilayah.
- Saat Anda meluncurkan WorkSpace, Anda harus memilih WorkSpace bundel. Sebuah paket adalah kombinasi dari sistem pengoperasian, dan penyimpanan, komputasi, dan sumber daya perangkat lunak. Untuk informasi selengkapnya, lihat Amazon WorkSpaces Bundles.
- Buat virtual private cloud dengan setidaknya dua subnet privat. Untuk informasi selengkapnya, lihat Konfigurasikan VPC untuk WorkSpaces. VPC harus terhubung ke jaringan on-premise Anda melalui hubungan jaringan pribadi virtual (VPN) atau AWS Direct Connect. Untuk informasi selengkapnya, lihat Prasyarat AD Connector dalam Panduan Administrasi AWS Directory Service.
- Menyediakan akses ke internet dari WorkSpace. Untuk informasi selengkapnya, lihat Menyediakan akses internet dari Anda WorkSpace.

Langkah 1: Buat AD Connector

> **Note**
>
> AD Connector tersedia untuk Anda secara gratis untuk digunakan WorkSpaces. Jika tidak ada yang WorkSpaces digunakan dengan direktori AD Connector Anda selama 30 hari berturut-turut, direktori ini akan secara otomatis dideregistrasi untuk digunakan dengan

Amazon WorkSpaces, dan Anda akan dikenakan biaya untuk direktori ini sesuai ketentuan harga. AWS Directory Service

Untuk menghapus direktori kosong, lihat Hapus direktori untuk WorkSpaces. Jika Anda menghapus direktori AD Connector, Anda selalu dapat membuat yang baru ketika Anda ingin mulai menggunakan WorkSpaces lagi.

Untuk membuat AD Connector

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih Siapkan Direktori, Buat AD Connector.
4. Untuk nama Organisasi, masukkan nama organisasi unik untuk direktori Anda (misalnya, my-example-directory). Nama ini harus terdiri dari setidaknya empat karakter, hanya terdiri dari karakter alfanumerik dan tanda hubung (-), dan dimulai atau diakhiri dengan karakter selain tanda hubung.
5. Untuk DNS Direktori Terhubung, masukkan nama direktori on-premise Anda yang memenuhi syarat (misalnya, example.com).
6. Untuk Nama NetBIOS direktori Terhubung, masukkan nama pendek direktori on-premise Anda (misalnya, example).
7. Untuk Nama pengguna akun konektor, masukkan nama pengguna dari pengguna di direktori on-premise Anda. Pengguna harus memiliki izin untuk membaca pengguna dan grup, membuat objek komputer, dan bergabung dengan komputer ke domain.
8. Untuk kata sandi akun Connector dan Konfirmasi kata sandi, masukkan kata sandi untuk pengguna lokal.
9. Untuk Alamat DNS, masukkan alamat IP setidaknya satu server DNS di direktori on-premise Anda.

   Important

   Jika Anda perlu memperbarui alamat IP server DNS Anda setelah meluncurkan Anda WorkSpaces, ikuti prosedur Perbarui server DNS untuk Amazon WorkSpaces untuk memastikan bahwa WorkSpaces Anda diperbarui dengan benar.
10. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk direktori.
11. Pertahankan Ukuran sebagai Kecil.

12. Untuk VPC, pilih VPC Anda.
13. Untuk Subnet, pilih subnet Anda. Server DNS yang Anda tentukan harus dapat diakses dari setiap subnet.
14. Pilih Langkah Selanjutnya.
15. Pilih Buat AD Connector. Dibutuhkan beberapa menit agar direktori Anda terhubung. Status awal dari direktori adalah `Requested` lalu `Creating`. Ketika pembuatan direktori selesai, statusnya adalah `Active`.

Langkah 2: Buat WorkSpace

Sekarang Anda siap meluncurkan WorkSpaces untuk satu atau beberapa pengguna di direktori lokal Anda.

Untuk meluncurkan WorkSpace untuk pengguna yang sudah ada

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih Luncurkan WorkSpaces.
4. Untuk Direktori, pilih direktori yang Anda buat.
5. (Opsional) Jika ini adalah pertama kalinya Anda meluncurkan WorkSpace di direktori ini, dan Amazon WorkDocs didukung di Wilayah, Anda dapat mengaktifkan atau menonaktifkan Amazon WorkDocs untuk semua pengguna di direktori. Untuk informasi selengkapnya tentang Amazon WorkDocs, lihat Amazon WorkDocs Drive di Panduan WorkDocs Administrasi Amazon.
6. Pilih Berikutnya. WorkSpaces mendaftarkan AD Connector Anda.
7. Pilih satu atau beberapa pengguna yang sudah ada dari direktori on-premise Anda. Jangan menambahkan pengguna baru ke direktori lokal melalui WorkSpaces konsol.

   Untuk menemukan pengguna untuk dipilih, Anda dapat memasukkan semua atau sebagian nama pengguna dan pilih Cari atau pilih Tampilkan Semua Pengguna. Perhatikan bahwa Anda tidak dapat memilih pengguna yang tidak memiliki alamat email.

   Setelah Anda memilih pengguna, pilih Tambahkan yang Dipilih lalu pilih Langkah Selanjutnya.
8. Di bawah Pilih Bundel, pilih WorkSpace bundel default yang akan digunakan untuk WorkSpaces. Di bawah Tetapkan WorkSpace Bundel, Anda dapat memilih bundel yang berbeda untuk individu WorkSpace jika diperlukan. Setelah Anda selesai, pilih Langkah Selanjutnya.

> **Note**
>
> Tinjau penggunaan dan spesifikasi yang disarankan dari setiap bundel untuk membantu memastikan Anda memilih bundel yang paling sesuai untuk pengguna Anda. Untuk informasi selengkapnya tentang setiap kasus penggunaan, lihat Amazon WorkSpaces Bundles. Untuk informasi selengkapnya tentang spesifikasi bundel, penggunaan yang disarankan, dan harga, lihat WorkSpaces harga Amazon.

9. Pilih mode berjalan untuk Anda WorkSpaces dan kemudian pilih Langkah Berikutnya. Untuk informasi selengkapnya, lihat Kelola mode WorkSpace berjalan.
10. Pilih Luncurkan WorkSpaces. Status awal dari WorkSpace adalah`PENDING`. Saat peluncuran selesai, statusnya adalah `AVAILABLE`.
11. Kirim undangan ke alamat email untuk setiap pengguna. (Undangan ini tidak dikirim secara otomatis jika Anda menggunakan AD Connector.) Untuk informasi selengkapnya, lihat Kirim email undangan.

Langkah 3: Connect ke WorkSpace

Anda dapat terhubung ke Anda WorkSpace menggunakan klien pilihan Anda. Setelah Anda masuk, klien akan menampilkan WorkSpace desktop.

Untuk terhubung ke WorkSpace

1. Buka tautan di email undangan.
2. Tinjau WorkSpaces Klien di Panduan WorkSpaces Pengguna Amazon untuk informasi selengkapnya tentang persyaratan untuk setiap klien, lalu lakukan salah satu hal berikut:
   - Saat diminta, unduh salah satu aplikasi client atau luncurkan Akses Web.
   - Jika Anda tidak diminta dan Anda belum menginstal aplikasi klien, buka https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

> **Note**
>
> Anda tidak dapat menggunakan browser web (Akses Web) untuk terhubung ke Amazon Linux WorkSpaces.

3. Mulai client, masukkan kode pendaftaran dari email undangan, dan pilih Daftar.
4. Saat diminta untuk masuk, masukkan kredenal masuk pengguna, lalu pilih Masuk.
5. (Opsional) Saat diminta untuk menyimpan kredensial Anda, pilih Ya.

> **Note**
>
> Karena Anda menggunakan AD Connector, pengguna Anda tidak akan dapat mengatur ulang kata sandi mereka sendiri. (Lupa kata sandi? pilihan pada layar login aplikasi WorkSpaces klien tidak akan tersedia.) Untuk informasi tentang cara mengatur ulang kata sandi pengguna, lihat Siapkan Alat Administrasi Direktori Aktif untuk WorkSpaces.

Langkah selanjutnya

Anda dapat terus menyesuaikan WorkSpace yang baru saja Anda buat. Misalnya, Anda dapat menginstal perangkat lunak dan kemudian membuat bundel khusus dari Anda WorkSpace. Anda juga dapat melakukan berbagai tugas administratif untuk WorkSpaces direktori Anda WorkSpaces dan Anda. Jika Anda selesai dengan Anda WorkSpace, Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat dokumentasi berikut.

- Buat WorkSpaces gambar dan bundel khusus
- Kelola Anda WorkSpaces
- Kelola direktori untuk WorkSpaces
- Menghapus WorkSpace

Untuk informasi selengkapnya tentang penggunaan aplikasi WorkSpaces klien, seperti menyiapkan beberapa monitor atau menggunakan perangkat periferal, lihat Dukungan WorkSpaces Klien dan Perangkat Periferal di Panduan WorkSpaces Pengguna Amazon.

Luncurkan WorkSpace menggunakan domain tepercaya

WorkSpaces memungkinkan Anda untuk menyediakan desktop Microsoft Windows, Amazon Linux, atau Ubuntu Linux virtual berbasis cloud untuk pengguna Anda, yang dikenal sebagai. WorkSpaces

WorkSpaces menggunakan direktori untuk menyimpan dan mengelola informasi untuk Anda WorkSpaces dan pengguna. Untuk direktori Anda, Anda dapat memilih dari Simple AD, AD

Connector, atau AWS Directory Service untuk Direktori Aktif, juga dikenal sebagai Microsoft AD Terkelola AWS. Selain itu, Anda dapat membangun hubungan kepercayaan antara direktori AWS Managed Microsoft AD dan domain on-premise Anda.

Dalam tutorial ini, kami meluncurkan WorkSpace yang menggunakan hubungan kepercayaan. Untuk tutorial yang menggunakan opsi lainnya, lihat Luncurkan desktop virtual menggunakan WorkSpaces.

Tugas

Sebelum Anda memulai

- Peluncuran WorkSpaces dengan Akun AWS domain tepercaya terpisah berfungsi dengan Microsoft AD yang AWS Dikelola saat dikonfigurasi dengan hubungan kepercayaan ke direktori lokal Anda. Namun, WorkSpaces menggunakan Simple AD atau AD Connector tidak dapat diluncurkan WorkSpaces untuk pengguna dari domain tepercaya.
- WorkSpaces tidak tersedia di setiap wilayah. Verifikasi Wilayah yang didukung dan pilih Wilayah untuk Anda WorkSpaces. Untuk informasi selengkapnya tentang Wilayah yang didukung, lihat WorkSpaces Harga menurut AWS Wilayah.
- Saat Anda meluncurkan WorkSpace, Anda harus memilih WorkSpace bundel. Sebuah paket adalah kombinasi dari sumber daya penyimpanan, komputasi, dan sumber daya perangkat lunak. Untuk informasi selengkapnya, lihat Amazon WorkSpaces Bundles.
- Saat Anda membuat direktori menggunakan AWS Directory Service atau meluncurkan WorkSpace, Anda harus membuat atau memilih cloud pribadi virtual yang dikonfigurasi dengan subnet publik dan dua subnet pribadi. Untuk informasi selengkapnya, lihat Konfigurasikan VPC untuk WorkSpaces.

Langkah 1: Bangun hubungan kepercayaan

Untuk mengatur hubungan kepercayaan

1. Siapkan Microsoft AD Terkelola AWS di virtual private cloud (VPC) Anda. Untuk informasi selengkapnya, lihat. Buat Direktori Microsoft AD terkelola AWS di AWS Directory Service Panduan Administrasi .

   > **Note**
   >
   > - Direktori bersama saat ini tidak didukung untuk digunakan dengan Amazon WorkSpaces.
   > - Jika direktori Microsoft AD AWS Terkelola Anda telah dikonfigurasi untuk replikasi Multi-wilayah, hanya direktori di Wilayah utama yang dapat didaftarkan untuk digunakan dengan Amazon. WorkSpaces Upaya untuk mendaftarkan direktori di Wilayah yang direplikasi untuk digunakan dengan Amazon WorkSpaces akan gagal. Replikasi Multi-Wilayah dengan AWS Microsoft AD Terkelola tidak didukung untuk digunakan dengan Amazon WorkSpaces dalam Wilayah yang direplikasi.

2. Buat hubungan kepercayaan antara perangkat Microsoft AD terkelola AWS dan domain on premise Anda. Pastikan bahwa kepercayaan dikonfigurasi sebagai kepercayaan dua arah. Untuk informasi selengkapnya, lihat. Tutorial: Buat Hubungan Kepercayaan Antara Microsoft AD terkelola AWS dan Domain on premise Anda di AWS Directory Service Panduan Administrasi .

Kepercayaan satu arah atau dua arah dapat digunakan untuk mengelola dan mengautentikasi WorkSpaces, sehingga WorkSpaces dapat disediakan untuk pengguna dan grup lokal. Untuk informasi selengkapnya, lihat Menerapkan Amazon WorkSpaces menggunakan Domain Sumber Daya Kepercayaan Satu Arah dengan AWS Directory Service.

> **Note**
>
> Ubuntu WorkSpaces menggunakan System Security Services Daemon (SSSD) untuk integrasi Active Directory, dan SSSD tidak mendukung kepercayaan hutan. Konfigurasikan kepercayaan eksternal sebagai gantinya. Kepercayaan dua arah direkomendasikan untuk Amazon Linux dan Ubuntu WorkSpaces.

Langkah 2: Buat WorkSpace

Setelah membuat hubungan kepercayaan antara iklan Microsoft AWS Terkelola dan domain Microsoft Active Directory lokal, Anda dapat menyediakan WorkSpaces untuk pengguna di domain lokal.

Perhatikan bahwa Anda harus memastikan bahwa pengaturan GPO direplikasi di seluruh domain sebelum Anda dapat menerapkannya. WorkSpaces

Cara meluncurkan workspaces bagi pengguna di domain on premise terpercaya

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih Luncurkan WorkSpaces.
4. Pada halaman Pilih Direktori, pilih direktori yang baru saja Anda daftarkan, lalu pilih Langkah Selanjutnya .
5. Di Identitas Pengguna, lakukan hal berikut:
   a. Untuk Pilih kepercayaan dari forest, pilih hubungan kepercayaan yang Anda buat.
   b. Pilih pengguna dari domain on premise, lalu pilih Tambahkan pilihan .
   c. Pilih Langkah Selanjutnya .
6. Pilih bundel yang akan digunakan untuk WorkSpaces dan kemudian pilih Langkah Berikutnya.

   > **Note**
   >
   > Tinjau penggunaan dan spesifikasi yang disarankan dari setiap bundel untuk membantu memastikan Anda memilih bundel yang paling sesuai untuk pengguna Anda. Untuk informasi selengkapnya tentang setiap kasus penggunaan, lihat Amazon WorkSpaces Bundles. Untuk informasi selengkapnya tentang spesifikasi bundel, penggunaan yang disarankan, dan harga, lihat WorkSpaces harga Amazon.

7. Pilih mode berjalan, pilih pengaturan enkripsi, dan konfigurasikan semua tanda. Setelah selesai, pilih Selanjutnya.
8. Pilih Luncurkan WorkSpaces. Perhatikan bahwa diperlukan waktu hingga 20 menit WorkSpaces agar tersedia, dan hingga 40 menit jika enkripsi diaktifkan. Status awal dari WorkSpace adalah`PENDING`. Saat peluncuran selesai, statusnya adalah `AVAILABLE`.

9. Kirim undangan ke alamat email untuk setiap pengguna. (Undangan ini tidak dikirim secara otomatis jika Anda menggunakan hubungan kepercayaan.) Untuk informasi selengkapnya, lihat Kirim email undangan.

Langkah 3: Connect ke WorkSpace

Setelah Anda menerima email undangan, Anda dapat terhubung ke email Anda WorkSpace. Pengguna dapat memasukkan nama pengguna mereka sebagai nama pengguna, corp\nama pengguna,\corp.example.com\nama pengguna).

Untuk terhubung ke WorkSpace

1. Buka tautan di email undangan. Saat diminta, masukkan kata sandi dan aktifkan pengguna. Ingat kata sandi ini karena Anda akan memerlukannya untuk masuk ke Anda WorkSpace.

   > **Note**
   >
   > Kata sandi peka terhadap huruf kapabilitas dan harus terdiri dari 8 hingga 64 karakter. Kata sandi harus berisi setidaknya satu karakter dari masing-masing kategori berikut: huruf kecil (a-z), huruf besar (A-Z), angka (0-9), dan ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.

2. Tinjau WorkSpaces Klien di Panduan WorkSpaces Pengguna Amazon untuk informasi selengkapnya tentang persyaratan untuk setiap klien, lalu lakukan salah satu hal berikut:

   - Saat diminta, unduh salah satu aplikasi client atau luncurkan Akses Web.
   - Jika Anda tidak diminta dan Anda belum menginstal aplikasi klien, buka https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

   > **Note**
   >
   > Anda tidak dapat menggunakan browser web (Akses Web) untuk terhubung ke Amazon Linux WorkSpaces.

3. Mulai client, masukkan kode pendaftaran dari email undangan, dan pilih Daftar.
4. Saat diminta untuk masuk, masukkan kredenal masuk pengguna, lalu pilih Masuk.
5. (Opsional) Saat diminta untuk menyimpan kredensial, pilih Ya.

Langkah selanjutnya

Anda dapat terus menyesuaikan WorkSpace yang baru saja Anda buat. Misalnya, Anda dapat menginstal perangkat lunak dan kemudian membuat bundel khusus dari Anda WorkSpace. Anda juga dapat melakukan berbagai tugas administratif untuk WorkSpaces direktori Anda WorkSpaces dan Anda. Jika Anda selesai dengan Anda WorkSpace, Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat dokumentasi berikut.

- Buat WorkSpaces gambar dan bundel khusus
- Kelola Anda WorkSpaces
- Kelola direktori untuk WorkSpaces
- Menghapus WorkSpace

Untuk informasi selengkapnya tentang penggunaan aplikasi WorkSpaces klien, seperti menyiapkan beberapa monitor atau menggunakan perangkat periferal, lihat Dukungan WorkSpaces Klien dan Perangkat Periferal di Panduan WorkSpaces Pengguna Amazon.

Mengelola pengguna WorkSpace

Masing-masing WorkSpace ditetapkan ke satu pengguna dan tidak dapat dibagikan oleh beberapa pengguna. Secara default, hanya satu WorkSpace per pengguna per direktori yang diizinkan.

Konten

Kelola WorkSpaces pengguna

Sebagai administrator untuk WorkSpaces, Anda dapat melakukan tugas-tugas berikut untuk mengelola WorkSpaces pengguna.

Edit informasi pengguna

Anda dapat menggunakan WorkSpaces konsol untuk mengedit informasi pengguna untuk file WorkSpace.

> **Note**
>
> Fitur ini hanya tersedia jika Anda menggunakan AWS Managed Microsoft AD atau Simple AD. Jika Anda menggunakan Microsoft Active Directory melalui AD Connector atau hubungan kepercayaan, Anda dapat mengelola pengguna dan grup menggunakan modul Active Directory.

Untuk mengedit informasi pengguna

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.

3. Pilih pengguna dan pilih Tindakan, Edit pengguna.
4. Perbarui Nama depan, Nama belakang, dan Email sesuai kebutuhan.
5. Pilih Update (Perbarui).

Tambahkan atau hapus pengguna

Anda dapat membuat pengguna dari WorkSpaces konsol Amazon hanya selama proses peluncuran WorkSpace, dan Anda tidak dapat menghapus pengguna melalui WorkSpaces konsol Amazon. Sebagian besar tugas manajemen pengguna, termasuk mengelola grup pengguna, harus dilakukan melalui direktori Anda.

Untuk menambah atau menghapus pengguna dan grup

Untuk menambah, menghapus, atau mengelola pengguna dan grup, Anda harus melakukannya melalui direktori Anda. Anda akan melakukan sebagian besar tugas administratif untuk WorkSpaces direktori Anda menggunakan alat manajemen direktori, seperti Alat Administrasi Direktori Aktif. Untuk informasi selengkapnya, lihat Siapkan Alat Administrasi Direktori Aktif untuk WorkSpaces.

> **Important**
>
> Sebelum Anda dapat menghapus pengguna, Anda harus menghapus yang WorkSpace ditetapkan untuk pengguna itu. Untuk informasi selengkapnya, lihat Menghapus WorkSpace.

Proses yang Anda gunakan untuk mengelola pengguna dan grup tergantung pada tipe direktori yang Anda gunakan.

- Jika Anda menggunakan Microsoft AD terkelola AWS, lihat Kelola Pengguna dan Grup di Microsoft AD terkelola AWS di Panduan Administrasi AWS Directory Service.
- Jika Anda menggunakan Simple AD, lihat Kelola Pengguna dan Grup di Simple AD di Panduan Administrasi AWS Directory Service.
- Jika Anda menggunakan Microsoft Active Directory melalui AD Connector atau hubungan kepercayaan, Anda dapat mengelola pengguna dan grup menggunakan modul Active Directory.

Kirim email undangan

Anda dapat mengirim email undangan ke pengguna secara manual jika diperlukan.

> **Note**
>
> Jika Anda menggunakan AD Connector atau domain tepercaya, email undangan tidak dikirim secara otomatis ke pengguna, jadi Anda harus mengirimkannya secara manual. Email undangan juga tidak dikirim secara otomatis jika pengguna sudah ada di Direktori Aktif.

Untuk mengirim ulang email undangan

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pada WorkSpaceshalaman, gunakan kotak pencarian untuk mencari pengguna yang ingin Anda kirimi undangan, lalu pilih yang sesuai WorkSpace dari hasil pencarian. Anda hanya dapat memilih satu WorkSpace per satu.
4. Pilih Tindakan, Undang pengguna.
5. Pada Undangan pengguna ke WorkSpace halaman, pilih Kirim undangan.

Buat beberapa WorkSpaces untuk pengguna

Secara default, Anda hanya dapat membuat satu WorkSpace per pengguna per direktori. Namun, jika diperlukan, Anda dapat membuat lebih dari satu WorkSpace untuk pengguna, tergantung pada pengaturan direktori Anda.

- Jika Anda hanya memiliki satu direktori untuk Anda WorkSpaces, buat beberapa nama pengguna untuk pengguna. Misalnya, pengguna bernama Mary Major dapat memiliki mmajor1, mmajor2, dan seterusnya sebagai nama pengguna. Setiap nama pengguna dikaitkan dengan yang berbeda WorkSpace dalam direktori yang sama, tetapi WorkSpaces memiliki kode registrasi yang sama, selama semua WorkSpaces dibuat di direktori yang sama di AWS Wilayah yang sama.
- Jika Anda memiliki beberapa direktori untuk Anda WorkSpaces, buat WorkSpaces untuk pengguna di direktori terpisah. Anda dapat menggunakan nama pengguna yang sama di direktori, atau Anda dapat menggunakan nama pengguna yang berbeda di direktori. WorkSpaces Akan memiliki kode pendaftaran yang berbeda.

> **Tip**
>
> Agar Anda dapat dengan mudah menemukan semua WorkSpaces yang telah Anda buat untuk pengguna, gunakan nama pengguna dasar yang sama untuk masing-masing WorkSpace.
> Misalnya, jika Anda memiliki pengguna bernama Mary Major dengan nama pengguna Active Directory mmajor, buat WorkSpaces untuknya dengan nama pengguna seperti mmajor, mmajor1, mmajor2, mmajor3, atau varian lain, seperti mmajor_windows atau mmajor_linux. Selama semua WorkSpaces memiliki nama pengguna dasar awal yang sama (mmajor), Anda dapat mengurutkan nama pengguna di WorkSpaces konsol Anda untuk mengelompokkan semua pengguna tersebut WorkSpaces bersama-sama.

> **Important**
>
> - Seorang pengguna dapat memiliki PCoIP dan WSP WorkSpace selama keduanya WorkSpaces berada di direktori terpisah. Pengguna yang sama tidak dapat memiliki PCoIP dan WSP WorkSpace di direktori yang sama.
> - Jika Anda menyiapkan beberapa WorkSpaces untuk digunakan dengan pengalihan lintas wilayah, Anda harus mengatur di direktori yang berbeda WorkSpaces di AWS Wilayah yang berbeda, dan Anda harus menggunakan nama pengguna yang sama di setiap direktori. Untuk informasi selengkapnya tentang pengalihan lintas wilayah, lihat Pengalihan Lintas Wilayah untuk Amazon WorkSpaces.

Untuk beralih di antara WorkSpaces, pengguna log in dengan nama pengguna dan kode registrasi yang terkait dengan Workspace tertentu. Jika pengguna menggunakan versi 3.0+ dari aplikasi WorkSpaces klien untuk Windows, macOS, atau Linux, pengguna dapat menetapkan nama yang berbeda WorkSpaces dengan masuk ke Pengaturan, Kelola Informasi Login di aplikasi klien.

Sesuaikan cara pengguna masuk ke mereka WorkSpaces

Sesuaikan akses pengguna Anda WorkSpaces dengan menggunakan pengidentifikasi sumber daya seragam (URI) untuk memberikan pengalaman login yang disederhanakan yang terintegrasi dengan alur kerja yang ada di organisasi Anda. Misalnya, Anda dapat secara otomatis menghasilkan

URI login yang mendaftarkan pengguna Anda dengan menggunakan kode WorkSpaces registrasi mereka. Hasilnya:

- Pengguna dapat melewati proses pendaftaran manual.
- Nama pengguna mereka secara otomatis dimasukkan pada halaman login WorkSpaces klien mereka.
- Jika otentikasi multi-faktor (MFA) digunakan di organisasi Anda, nama pengguna dan kode MFA mereka secara otomatis dimasukkan pada halaman login klien mereka.

Akses URI berfungsi pada kedua kode pendaftaran berbasis Wilayah (misalnya, `WSpdx+ABC12D`) dan kode pendaftaran berbasis nama domain yang memenuhi syarat (FQDN) (misalnya, `desktop.example.com`). Untuk informasi selengkapnya tentang membuat dan menggunakan kode pendaftaran berbasis FQDN, lihat Pengalihan Lintas Wilayah untuk Amazon WorkSpaces.

Anda dapat mengonfigurasi akses URI WorkSpaces untuk aplikasi klien pada perangkat yang didukung berikut:

- Komputer Windows
- Komputer macOS
- Ubuntu Linux 18.04, 20.04, dan 22.04 komputer
- iPad
- Perangkat android

Untuk menggunakan URI untuk mengakses mereka WorkSpaces, pengguna harus terlebih dahulu menginstal aplikasi klien untuk perangkat mereka dengan membuka https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

Akses URI didukung pada browser Firefox dan Chrome di komputer Windows dan macOS, di browser Firefox di komputer Ubuntu Linux 18.04, 20.04, dan 22.04, dan di Internet Explorer dan browser Microsoft Edge di komputer Windows. Untuk informasi selengkapnya tentang WorkSpaces klien, lihat WorkSpaces Klien di Panduan WorkSpaces Pengguna Amazon.

> **Note**
>
> Di perangkat Android, akses URI hanya berfungsi pada peramban Firefox, bukan dengan peramban Google Chrome.

Untuk mengonfigurasi akses URI ke WorkSpaces, gunakan salah satu format URI yang dijelaskan dalam tabel berikut.

> **Note**
>
> Jika komponen data URI Anda termasuk salah satu karakter reservasi berikut, sebaiknya gunakan pengodean persentase dalam komponen data untuk menghindari ambiguitas:
> `@ : / ? & =`
> Misalnya, jika Anda memiliki nama pengguna yang menyertakan salah satu karakter ini, Anda harus menyandikan persentase nama pengguna tersebut di URI Anda. Untuk informasi selengkapnya, lihat Pengidentifikasi Sumber Daya Seragam (URI): Generic Syntax.

Sintaksis yang didukung	Deskripsi
workspaces://	Membuka aplikasi WorkSpaces klien. (Catatan: Menggunakan workspaces:// dengan sendirinya saat ini tidak didukung dalam aplikasi klien Linux.)
workspaces://@registrationcode	Mendaftarkan pengguna dengan menggunakan kode WorkSpaces registrasi mereka. Juga menampilkan halaman masuk klien.
workspaces://username@registrationcode	Mendaftarkan pengguna dengan menggunakan kode WorkSpaces registrasi mereka. Juga secara otomatis memasukkan nama pengguna di bidang nama pengguna pada halaman login klien.
workspaces://username@registrationcode?MFACode=mfa	Mendaftarkan pengguna dengan menggunakan kode WorkSpaces registrasi mereka. Juga secara otomatis memasukkan nama pengguna di bidang nama pengguna dan kode otentikasi multi-faktor (MFA) di bidang kode MFA pada halaman login klien.
workspaces://@registrationcode?MFACode=mfa	Mendaftarkan pengguna dengan menggunakan kode WorkSpaces registrasi mereka. Juga secara otomatis memasukkan kode autentikasi multi-faktor (MFA) pada kolom Kode MFA di halaman masuk klien.

> **Note**
>
> Jika pengguna membuka tautan URI ketika mereka sudah terhubung ke klien WorkSpace dari Windows, WorkSpaces sesi baru terbuka dan WorkSpaces sesi aslinya tetap terbuka. Jika pengguna membuka tautan URI saat terhubung ke klien macOS, iPad, atau Android, tidak ada sesi baru yang terbuka; hanya WorkSpaces sesi aslinya yang tetap terbuka. WorkSpace

Aktifkan kemampuan WorkSpace manajemen swalayan untuk pengguna Anda

Di WorkSpaces, Anda dapat mengaktifkan kemampuan WorkSpace manajemen swalayan bagi pengguna Anda untuk memberi mereka kontrol lebih besar atas pengalaman mereka. Ini juga dapat mengurangi beban kerja staf dukungan TI Anda. WorkSpaces Saat Anda mengaktifkan kemampuan swalayan, pengguna dapat melakukan satu atau lebih tugas berikut langsung dari WorkSpaces klien mereka:

- Cache kredensial pada klien mereka. Ini memungkinkan mereka terhubung kembali ke mereka WorkSpace tanpa memasukkan kembali kredensialnya.
- Mulai ulang (reboot) mereka WorkSpace.
- Tingkatkan ukuran root dan volume pengguna pada mereka WorkSpace.
- Ubah jenis komputasi (bundel) untuk mereka WorkSpace.
- Ganti mode berjalan mereka WorkSpace.
- Membangun kembali mereka WorkSpace.

Klien yang didukung

- Android, berjalan pada Android atau sistem OS Chrome Android yang kompatibel
- Linux
- macOS
- Windows

Untuk mengaktifkan kemampuan manajemen layanan mandiri bagi pengguna Anda

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda, dan pilih Tindakan, Perbarui Detail.
4. Perluas Izin Layanan Mandiri Pengguna. Aktifkan atau nonaktifkan opsi berikut yang diperlukan untuk menentukan tugas WorkSpace manajemen yang dapat dilakukan pengguna dari klien mereka:

   - Ingat saya — Pengguna dapat memilih akan meng-cache kredensialnya pada klien mereka dengan memilih kotak centang Ingat Saya atau Biarkan saya tetap masuk pada layar masuk. Kredensial hanya di-cache di RAM. Ketika pengguna memilih untuk men-cache kredensialnya, mereka dapat terhubung kembali WorkSpaces tanpa memasukkan kembali kredensialnya. Untuk mengontrol berapa lama pengguna dapat meng-cache kredensialnya, lihat Atur masa pakai maksimum untuk tiket Kerberos.
   - Mulai ulang WorkSpace dari klien - Pengguna dapat memulai ulang (reboot) mereka WorkSpace. Memulai ulang memutus pengguna dari mereka WorkSpace, mematikannya, dan mem-boot ulang. Data pengguna, sistem operasi, dan pengaturan sistem tidak terpengaruh.
   - Meningkatkan ukuran volume — Pengguna dapat memperluas root dan volume pengguna WorkSpace ke ukuran tertentu tanpa menghubungi dukungan TI. Pengguna dapat meningkatkan ukuran volume root (untuk Windows, drive C:; untuk Linux,/) hingga 175 GB, dan ukuran volume pengguna (untuk Windows, drive D:; untuk Linux, /home) hingga 100 GB. WorkSpace root dan volume pengguna datang dalam grup set yang tidak dapat diubah. Grup yang tersedia adalah [Root(GB), User(GB)]: [80, 10], [80, 50], [80, 100], [175 to 2000, 100 hingga 2000]. Untuk informasi selengkapnya, lihat Memodifikasi WorkSpace.

     Untuk yang baru dibuat WorkSpace, pengguna harus menunggu 6 jam sebelum mereka dapat meningkatkan ukuran drive ini. Setelah itu, mereka bisa melakukannya hanya satu kali dalam periode 6 jam. Sementara peningkatan ukuran volume sedang berlangsung, pengguna dapat melakukan sebagian besar tugas pada mereka WorkSpace. Tugas yang tidak dapat mereka lakukan adalah: mengubah jenis WorkSpace komputasi mereka, mengganti mode WorkSpace berjalan mereka, memulai ulang WorkSpace, atau membangun kembali mereka. WorkSpace Ketika proses selesai, WorkSpace harus di-boot ulang agar perubahan diterapkan. Proses ini dapat memakan waktu hingga satu jam.

> **Note**
>
> Jika pengguna meningkatkan ukuran volume pada mereka WorkSpace, ini meningkatkan tingkat penagihan untuk mereka WorkSpace.

- Ubah jenis komputasi — Pengguna dapat beralih di WorkSpace antara jenis komputasi (bundel). Untuk yang baru dibuat WorkSpace, pengguna harus menunggu 6 jam sebelum mereka dapat beralih ke bundel yang berbeda. Setelah itu, mereka dapat beralih ke paket yang lebih besar hanya satu kali dalam periode 6 jam, atau ke paket yang lebih kecil satu kali dalam periode 30 hari. Ketika perubahan jenis WorkSpace komputasi sedang berlangsung, pengguna terputus dari mereka WorkSpace, dan mereka tidak dapat menggunakan atau mengubah. WorkSpace Secara otomatis reboot selama proses perubahan jenis komputasi. WorkSpace Proses ini dapat memakan waktu hingga satu jam.

  > **Note**
  >
  > Jika pengguna mengubah jenis WorkSpace komputasi mereka, ini mengubah tingkat penagihan untuk mereka. WorkSpace

- Beralih mode berjalan - Pengguna dapat beralih WorkSpace antara mode AlwaysOndan mode yang AutoStopsedang berjalan. Untuk informasi selengkapnya, lihat Kelola mode WorkSpace berjalan.

  > **Note**
  >
  > Jika pengguna beralih mode berjalan mereka WorkSpace, ini mengubah tingkat penagihan untuk mereka WorkSpace.

- Membangun kembali WorkSpace dari klien — Pengguna dapat membangun kembali sistem operasi dari a WorkSpace ke keadaan semula. Ketika a WorkSpace dibangun kembali, volume pengguna (D: drive) dibuat ulang dari cadangan terbaru. Karena pencadangan selesai setiap 12 jam, data pengguna mungkin berusia hingga 12 jam. Untuk yang baru dibuat WorkSpace, pengguna harus menunggu 12 jam sebelum mereka dapat membangun kembali mereka WorkSpace. Ketika WorkSpace pembangunan kembali sedang berlangsung, pengguna terputus dari mereka WorkSpace, dan mereka tidak dapat menggunakan atau membuat perubahan pada mereka. WorkSpace Proses ini dapat memakan waktu hingga satu jam.

5. Pilih Perbarui atau Perbarui dan Keluar.

Aktifkan pengoptimalan audio Amazon Connect untuk pengguna Anda

Di konsol WorkSpaces manajemen, Anda dapat mengaktifkan pengoptimalan audio Amazon Connect Contact Control Panel (CCP) untuk WorkSpaces armada Anda guna meningkatkan keamanan dan mengaktifkan audio berkualitas asli. Setelah mengaktifkan pengoptimalan audio CCP, audio CCP akan diproses oleh titik akhir klien, sementara WorkSpaces pengguna dapat berinteraksi dengan PKC dari dalam mereka. WorkSpaces

Pengoptimalan audio Amazon Connect Contact Control Panel (CCP) berfungsi dengan:

- Klien WorkSpaces Windows.
- Amazon Linux dan Windows WorkSpaces.
- WorkSpaces menggunakan PCoIP atau WSP.

Persyaratan

- Anda harus diatur dengan Amazon Connect.
- Anda harus membuat CCP khusus dengan Amazon Connect Stream API dengan membuat CCP tanpa media untuk pensinyalan panggilan. Dengan cara ini, media ditangani di desktop lokal menggunakan CCP standar, dan kontrol pensinyalan dan panggilan ditangani pada koneksi jarak jauh dengan PKC tanpa media. Untuk informasi selengkapnya tentang Amazon Connect stream API, lihat GitHub repositori di. https://github.com/aws/amazon-connect-streams PKT khusus yang Anda buat adalah PKT yang akan digunakan agen Amazon Connect Anda di dalamnya. WorkSpaces
- Anda harus memasang browser web ke titik akhir WorkSpaces klien yang didukung oleh Amazon Connect. Untuk daftar browser yang didukung, lihat Browser yang didukung oleh Amazon Connect.

> **Note**
>
> Jika pengguna Anda menggunakan browser yang tidak didukung, mereka akan diminta untuk mengunduh browser yang didukung saat mereka mencoba masuk ke PKC.

Aktifkan optimasi audio Amazon Connect

Untuk mengaktifkan pengoptimalan audio Amazon Connect bagi pengguna Anda:

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda, dan pilih Tindakan, Perbarui Detail.
4. Perluas Optimasi Audio Amazon Connect.

> **Note**
>
> Sebelum mengonfigurasi dengan Amazon Connect, pilih Perbarui untuk menyimpan perubahan yang belum disimpan yang dibuat sebelumnya di konsol manajemen.

5. Pilih Konfigurasikan Amazon Connect.
6. Masukkan nama Panel Kontrol Kontak Amazon Connect (CCP).

> **Note**
>
> Nama yang Anda berikan kepada CCP Anda akan digunakan di menu add-in pengguna. Pilih nama yang akan berarti bagi pengguna Anda.

7. Masukkan URL Panel Kontrol Kontak Amazon Connect yang dihasilkan oleh Amazon Connect. Lihat Menyediakan akses ke Contact Control Panel untuk informasi selengkapnya tentang mendapatkan URL.
8. Pilih Buat Amazon Connect.

Perbarui detail pengoptimalan audio Amazon Connect direktori

Untuk memperbarui detail pengoptimalan audio Amazon Connect direktori:

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda, dan pilih Tindakan, Perbarui Detail.
4. Perluas Optimasi Audio Amazon Connect.

> **Note**
>
> Sebelum mengonfigurasi dengan Amazon Connect, pilih Perbarui untuk menyimpan perubahan yang belum disimpan yang dibuat sebelumnya di konsol manajemen.

5. Pilih Konfigurasikan Amazon Connect.
6. Pilih Edit.
7. Pilih direktori Anda, dan pilih Tindakan, Perbarui Detail.
8. Perbarui nama dan URL Panel Kontrol Kontak Amazon Connect.
9. Pilih Save (Simpan).

Hapus pengoptimalan audio Amazon Connect direktori

Untuk menghapus optimasi audio Amazon Connect direktori:

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda, dan pilih Tindakan, Perbarui Detail.
4. Perluas Optimasi Audio Amazon Connect.

> **Note**
>
> Sebelum mengonfigurasi dengan Amazon Connect, pilih Perbarui untuk menyimpan perubahan yang belum disimpan yang dibuat sebelumnya di konsol manajemen.

5. Pilih Konfigurasikan Amazon Connect.
6. Pilih Hapus Amazon Connect.

Lihat panduan pelatihan Agen untuk informasi lebih lanjut.

Aktifkan unggahan log diagnostik

Untuk memecahkan masalah WorkSpaces klien, aktifkan unggahan log diagnostik otomatis. Ini saat ini didukung untuk klien Windows, macOS, Linux, dan Web Access.

> **Note**
>
> Fitur unggahan log diagnostik WorkSpaces klien saat ini tidak tersedia di Wilayah AWS GovCloud (AS-Barat).

Unggahan log diagnostik

Dengan unggahan log Diagnostik, Anda dapat mengunggah file log WorkSpaces klien langsung WorkSpaces ke untuk memecahkan masalah tanpa mengganggu penggunaan klien. WorkSpaces Jika Anda mengaktifkan unggahan log diagnostik untuk pengguna Anda, atau membiarkan pengguna melakukannya sendiri, file log akan dikirim secara WorkSpaces otomatis. Anda dapat mengaktifkan unggahan log diagnostik sebelum atau selama sesi WorkSpaces streaming.

Untuk mengunggah log diagnostik secara otomatis dari perangkat yang dikelola, instal WorkSpaces klien yang mendukung unggahan diagnostik. Pengunggahan log diaktifkan secara default. Anda dapat mengubah pengaturan dengan salah satu cara berikut:

Opsi 1: Menggunakan AWS konsol

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih nama direktori yang ingin Anda aktifkan pencatatan diagnostik.
4. Gulir ke bawah ke izin layanan mandiri.
5. Pilih Edit.
6. Pilih Unggahan log diagnostik.
7. Pilih Simpan.

Opsi 2: Menggunakan panggilan API

Anda dapat mengedit pengaturan direktori untuk mengaktifkan atau menonaktifkan klien WorkSpaces Windows, macOS, dan Linux untuk mengunggah log diagnostik secara otomatis menggunakan panggilan API. Jika diaktifkan, ketika masalah klien terjadi, log dikirim ke WorkSpaces tanpa interaksi pengguna. Untuk informasi selengkapnya, lihat referensi WorkSpaces API.

Anda juga dapat membiarkan pengguna Anda memilih apakah akan mengaktifkan unggahan log diagnostik otomatis setelah instalasi klien. Untuk informasi selengkapnya, lihat Aplikasi klien WorkSpaces Windows, aplikasi klien WorkSpaces macOS, dan aplikasi klien WorkSpaces Linux.

> **Note**
>
> - Log diagnostik tidak mengandung informasi sensitif. Anda dapat menonaktifkan unggahan log diagnostik otomatis untuk pengguna Anda di tingkat direktori, atau mengizinkan pengguna Anda menonaktifkan fitur ini sendiri.
> - Untuk mengakses fitur unggahan log diagnostik, Anda perlu menginstal versi WorkSpaces klien berikut:
>   - 5.4.0 atau yang lebih baru dari klien Windows
>   - 5.8.0 atau yang lebih baru dari klien macOS
>   - 2023.1 dari klien Ubuntu 22.04
>   - 2023.1 dari klien Ubuntu 20.04
>   - Anda juga dapat mengakses fitur unggah log diagnostik dengan klien Akses Web

Kelola Anda WorkSpaces

Anda dapat mengelola Anda WorkSpaces menggunakan WorkSpaces konsol.

Untuk melakukan tugas administrasi direktori, lihat the section called “Siapkan Administrasi direktori”.

> **Note**
>
> - Pastikan Anda memperbarui driver ketergantungan jaringan seperti driver ENA, NVMe, dan PV pada Anda. WorkSpaces Anda harus melakukan ini setidaknya sekali setiap 6 bulan. Untuk informasi selengkapnya, lihat Menginstal atau memutakhirkan driver Elastic Network Adapter (ENA), Driver AWS NVMeuntuk instance Windows, dan Upgrade driver PV pada instans Windows.
> - Pastikan Anda memperbarui agen EC2config, EC2launch, dan EC2launch V2 ke versi terbaru secara berkala. Anda harus melakukan ini setidaknya sekali setiap 6 bulan. Untuk informasi selengkapnya, lihat Memperbarui EC2config dan EC2launch.

Konten

- Microsoft 365 Bawa Lisensi Anda Sendiri (BYOL)
- Tingkatkan Windows BYOL WorkSpaces
- Migrasi a WorkSpace
- Menghapus WorkSpace

Kelola Windows Anda WorkSpaces

Anda dapat menggunakan Objek Kebijakan Grup (GPO) untuk menerapkan pengaturan untuk mengelola Windows WorkSpaces atau pengguna yang merupakan bagian dari WorkSpaces direktori Windows Anda.

> **Note**
>
> Instans Linux tidak mematuhi Kebijakan Grup. Untuk informasi tentang mengelola Amazon Linux WorkSpaces, lihatKelola Amazon Linux Anda WorkSpaces.

Kami menyarankan Anda membuat unit organisasi untuk Objek WorkSpaces Komputer Anda dan unit organisasi untuk Objek WorkSpaces Pengguna Anda.

Untuk menggunakan pengaturan Kebijakan Grup yang khusus untuk Amazon WorkSpaces, Anda harus menginstal template administratif Kebijakan Grup untuk protokol atau protokol yang Anda gunakan, baik PCoIP atau WorkSpaces Streaming Protocol (WSP).

> **Warning**
>
> Pengaturan Kebijakan Grup dapat memengaruhi pengalaman WorkSpace pengguna Anda sebagai berikut:
>
> - Menerapkan pesan logon interaktif untuk menampilkan banner logon mencegah pengguna untuk dapat mengakses mereka. WorkSpaces Pengaturan Kebijakan Grup pesan masuk interaktif saat ini tidak didukung oleh WorkSpaces.
> - Menonaktifkan penyimpanan yang dapat dilepas melalui pengaturan Kebijakan Grup menyebabkan kegagalan masuk yang mengakibatkan pengguna log in ke profil pengguna sementara tanpa akses ke drive D.
> - Menghapus pengguna dari grup lokal Pengguna Desktop Jarak Jauh melalui pengaturan Kebijakan Grup mencegah pengguna tersebut untuk dapat mengautentikasi melalui

aplikasi WorkSpaces klien. Untuk informasi selengkapnya tentang pengaturan Kebijakan Grup ini, lihat Izinkan log on melalui Layanan Desktop Jarak Jauhdalam dokumentasi Microsoft.

- Jika Anda menghapus grup Pengguna bawaan dari kebijakan keamanan lokal Allow log on, WorkSpaces pengguna PCoIP Anda tidak akan dapat terhubung ke grup tersebut WorkSpaces WorkSpaces melalui aplikasi klien. PCoIP Anda WorkSpaces juga tidak akan menerima pembaruan untuk perangkat lunak agen PCoIP. Pembaruan agen PCoIP mungkin berisi keamanan dan perbaikan lainnya, atau mereka mungkin mengaktifkan fitur baru untuk Anda. WorkSpaces Untuk informasi selengkapnya tentang bekerja dengan kebijakan keamanan ini, lihat Izinkan log on secara lokal di dalam dokumentasi Microsoft.
- Pengaturan Kebijakan Grup dapat digunakan untuk membatasi akses drive. Jika Anda mengonfigurasi pengaturan Kebijakan Grup untuk membatasi akses ke drive C atau drive D, pengguna tidak dapat mengaksesnya WorkSpaces. Untuk mencegah masalah ini terjadi, pastikan bahwa pengguna Anda dapat mengakses drive C dan drive D.
- Fitur WorkSpaces audio-in memerlukan akses masuk lokal di dalam file. WorkSpace Fitur audio-in diaktifkan secara default untuk Windows. WorkSpaces Namun, jika Anda memiliki setelan Kebijakan Grup yang membatasi logon lokal pengguna di dalamnya WorkSpaces, audio-in tidak akan berfungsi pada Anda. WorkSpaces Jika Anda menghapus setelan Kebijakan Grup itu, fitur audio-in diaktifkan setelah reboot berikutnya. WorkSpace Untuk informasi selengkapnya tentang pengaturan Kebijakan Grup ini, lihat Izinkan log on secara lokal dalam dokumentasi Microsoft.

  Untuk informasi selengkapnya tentang mengaktifkan atau menonaktifkan audio-in, lihat Aktifkan atau nonaktifkan pengalihan audio-in untuk PCoIP atau Aktifkan atau nonaktifkan pengalihan audio-in untuk WSP.
- Menggunakan Kebijakan Grup untuk mengatur paket daya Windows ke Balanced atau Power saver dapat WorkSpaces menyebabkan Anda tertidur ketika mereka dibiarkan menganggur. Kami sangat merekomendasikan untuk menggunakan Kebijakan Grup guna mengatur rencana daya Windows ke Performa tinggi. Untuk informasi selengkapnya, lihat WorkSpace Jendela saya tertidur ketika dibiarkan menganggur.
- Beberapa pengaturan Kebijakan Grup memaksa para pengguna untuk log off saat mereka terputus dari sesi. Aplikasi apa pun yang dibuka pengguna WorkSpaces ditutup.
- “Setel batas waktu untuk sesi Layanan Desktop Jarak Jauh yang aktif tetapi tidak aktif” saat ini tidak didukung di WorkSpaces WSP. Hindari menggunakannya selama sesi WSP karena menyebabkan pemutusan bahkan ketika ada aktivitas dan sesi tidak menganggur.

Untuk informasi tentang menggunakan alat administrasi Direktori Aktif untuk bekerja dengan GPO, lihat Siapkan Alat Administrasi Direktori Aktif untuk WorkSpaces.

Daftar Isi

Instal file template administratif Kebijakan Grup untuk Protokol WorkSpaces Streaming (WSP)

Untuk menggunakan pengaturan Kebijakan Grup yang khusus untuk WorkSpaces saat menggunakan Protokol WorkSpaces Streaming (WSP), Anda harus menambahkan template administratif Kebijakan Grup `wsp.admx` dan `wsp.adml` file untuk WSP ke Central Store pengontrol domain untuk direktori Anda WorkSpaces . Untuk informasi selengkapnya tentang file `.admx` dan `.adml`, lihat Cara membuat dan mengelola Penyimpanan Pusat untuk Templat Administratif Kebijakan Grup di Windows.

Prosedur berikut menjelaskan cara membuat Penyimpanan Pusat dan menambahkan file templat administratif ke dalamnya. Lakukan prosedur berikut pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke direktori Anda WorkSpaces.

Untuk menginstal file templat administratif Kebijakan Grup untuk WSP

1. Dari Windows yang sedang berjalan WorkSpace, buat salinan `wsp.adml` file `wsp.admx` dan file di `C:\Program Files\Amazon\WSP` direktori.

2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka Windows File Explorer, dan di bilah alamat, masukkan nama domain yang memenuhi syarat penuh (FQDN) organisasi Anda, seperti. `\\example.com`
3. Buka folder `sysvol`.
4. Buka folder dengan nama *FQDN*.
5. Buka folder `Policies`. Anda sekarang seharusnya berada di `\\`*FQDN*`\sysvol\`*FQDN*`\Policies`.
6. Jika belum ada, buat folder dengan nama `PolicyDefinitions`.
7. Buka folder `PolicyDefinitions`.
8. Salin file `wsp.admx` ke dalam folder `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions`.
9. Buat folder dengan nama `en-US` di dalam folder `PolicyDefinitions`.
10. Buka folder `en-US`.
11. Salin file `wsp.adml` ke dalam folder `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions\en-US`.

Untuk memverifikasi bahwa file templat administratif diinstal dengan benar

1. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
2. Perluas forest (Forest:***FQDN***).
3. Perluas Domain.
4. Perluas FQDN Anda (misalnya, `example.com`).
5. Perluas Objek Kebijakan Grup.
6. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebaliknya, Anda harus membuat dan menautkan GPO di bawah kontainer domain yang memiliki hak istimewa yang didelegasikan.
> Saat Anda membuat direktori dengan AWS Managed Microsoft AD, AWS Directory Service buat unit organisasi *yourdomainname* (OU) di bawah root domain. Nama OU

ini didasarkan pada nama NetBIOS yang Anda ketik saat membuat direktori Anda. Jika Anda tidak menentukan nama NetBIOS, nama tersebut akan default ke bagian pertama dari nama DNS Direktori Anda (misalnya, dalam kasus `corp.example.com`, nama NetBIOS adalah `corp`).
Untuk membuat GPO Anda, alih-alih memilih Kebijakan Domain Default, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini.
Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

7. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
8. Anda sekarang dapat menggunakan objek Kebijakan Grup WSP ini untuk memodifikasi pengaturan Kebijakan Grup yang khusus untuk WorkSpaces saat menggunakan WSP.

Mengelola pengaturan Kebijakan Grup untuk Protokol WorkSpaces Streaming (WSP)

Gunakan pengaturan Kebijakan Grup untuk mengelola Windows Anda WorkSpaces yang menggunakan WSP.

Konfigurasikan dukungan printer untuk WSP

Secara default, WorkSpaces memungkinkan pencetakan jarak jauh Dasar, yang menawarkan kemampuan pencetakan terbatas karena menggunakan driver printer generik di sisi host untuk memastikan pencetakan yang kompatibel.

Pencetakan jarak jauh lanjutan untuk client Windows (tidak tersedia untuk WSP) memungkinkan Anda menggunakan fitur khusus pada printer Anda, seperti pencetakan dua sisi, tetapi memerlukan instalasi driver printer yang cocok di sisi host.

Pencetakan jarak jauh diimplementasikan sebagai saluran virtual. Jika saluran virtual dinonaktifkan, pencetakan jarak jauh tidak berfungsi.

Untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk mengonfigurasi dukungan printer sesuai kebutuhan.

Untuk mengonfigurasi dukungan printer

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Konfigurasikan pencetakan jarak jauh.
10. Di kotak dialog Konfigurasikan pencetakan jarak jauh, lakukan salah satu hal berikut:
    - Untuk mengaktifkan pengalihan printer lokal, pilih Diaktifkan, lalu untuk Opsi pencetakan, pilih Dasar. Untuk secara otomatis menggunakan printer default komputer client saat ini, pilih Petakan printer default lokal ke host jarak jauh.
    - Untuk menonaktifkan pencetakan, pilih Dinonaktifkan.
11. Pilih OKE.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

- Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
- Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Konfigurasikan pengalihan clipboard untuk WSP

Secara default, WorkSpaces mendukung pengalihan clipboard dua arah (salin/tempel). Untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini atau mengonfigurasi arah di mana pengalihan clipboard diizinkan.

Untuk mengkonfigurasi pengalihan clipboard untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Konfigurasikan pengalihan clipboard.
10. Dalam kotak dialog Konfigurasi pengalihan clipboard, pilih Diaktifkan atau Dinonaktifkan.

Saat Konfigurasi pengalihan clipboard Diaktifkan, opsi pengalihan Clipboard berikut akan tersedia:

- Pilih Salin dan Tempel untuk memungkinkan pengalihan salin dan tempel clipboard dua arah.
- Pilih Salin Hanya untuk mengizinkan penyalinan data dari clipboard server ke clipboard klien saja.
- Pilih Tempel Hanya untuk memungkinkan menempelkan data dari clipboard klien ke clipboard server saja.

11. Pilih OK.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

    - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Pembatasan yang diketahui

Dengan pengalihan clipboard diaktifkan pada WorkSpace, jika Anda menyalin konten yang lebih besar dari 890 KB dari aplikasi Microsoft Office, aplikasi mungkin menjadi lambat atau tidak responsif hingga 5 detik.

Setel batas waktu melanjutkan sesi untuk WSP

Ketika Anda kehilangan konektivitas jaringan, sesi WorkSpaces klien aktif Anda terputus. WorkSpaces aplikasi klien untuk Windows dan macOS mencoba menghubungkan kembali sesi secara otomatis jika konektivitas jaringan dipulihkan dalam jangka waktu tertentu. Batas waktu resume sesi default adalah 20 menit (1200 detik), tetapi Anda dapat mengubah nilai WorkSpaces tersebut untuk yang dikendalikan oleh pengaturan Kebijakan Grup domain Anda.

Untuk mengatur nilai batas waktu melanjutkan sesi otomatis

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.

3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan/nonaktifkan menghubungkan ulang otomatis.
10. Di kotak dialog Aktifkan/nonaktifkan menghubungkan ulang otomatis, pilih Diaktifkan, lalu atur Batas waktu menghubungkan ulang (detik) ke batas waktu yang diinginkan dalam detik.
11. Pilih OKE.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
    - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Aktifkan atau nonaktifkan pengalihan video-in untuk WSP

Secara default, WorkSpaces mendukung pengalihan data dari kamera lokal. Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

Untuk mengaktifkan atau menonaktifkan pengalihan video-in untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

   > **Note**
   >
   > Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .
8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan/nonaktifkan pengalihan video-in.
10. Di kotak dialog Aktifkan/nonaktifkan pengalihan video-in, pilih Diaktifkan atau Dinonaktifkan.
11. Pilih OKE.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

    - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Aktifkan atau nonaktifkan pengalihan audio-in untuk WSP

Secara default, WorkSpaces mendukung pengalihan data dari mikrofon lokal. Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

Untuk mengaktifkan atau menonaktifkan pengalihan audio-in untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan/nonaktifkan pengalihan audio-in.
10. Di kotak dialog Aktifkan/nonaktifkan pengalihan audio-in, pilih Diaktifkan atau Dinonaktifkan.
11. Pilih OKE.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

- Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
- Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Mengaktifkan atau menonaktifkan pengalihan audio-out untuk WSP

Secara default, WorkSpaces mengalihkan data ke pembicara lokal. Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

Untuk mengaktifkan atau menonaktifkan pengalihan audio-out untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda. Misalnya, `example.com`.
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan/nonaktifkan pengalihan audio-out.
10. Dalam kotak dialog Aktifkan/nonaktifkan pengalihan audio keluar, pilih Diaktifkan atau Dinonaktifkan.

11. Pilih OK.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
    - Nyalakan ulang WorkSpace. Di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan > Reboot WorkSpaces.
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Nonaktifkan pengalihan zona waktu untuk WSP

Secara default, waktu dalam Workspace diatur untuk mencerminkan zona waktu klien yang digunakan untuk terhubung ke WorkSpace. Perilaku ini dikendalikan melalui pengalihan zona waktu. Anda mungkin ingin mematikan arah zona waktu karena berbagai alasan. Sebagai contoh:

- Perusahaan Anda ingin semua karyawan bekerja di zona waktu tertentu (bahkan jika beberapa karyawan berada di zona waktu yang lain).
- Anda telah menjadwalkan tugas dalam WorkSpace yang dimaksudkan untuk dijalankan pada waktu tertentu di zona waktu tertentu.
- Pengguna Anda yang sering bepergian ingin mempertahankan zona waktu mereka WorkSpaces dalam satu zona waktu untuk konsistensi dan preferensi pribadi.

Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

Untuk menonaktifkan pengalihan zona waktu untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.

7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *yourdomainname*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *yourdomainname*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan/nonaktifkan pengalihan zona waktu.
10. Di kotak dialog Aktifkan/nonaktifkan pengalihan zona waktu, pilih Dinonaktifkan.
11. Pilih OKE.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
    - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.
13. Atur zona waktu untuk WorkSpaces ke zona waktu yang diinginkan.

Zona waktu sekarang statis dan tidak lagi mencerminkan zona waktu mesin klien. WorkSpaces

Konfigurasikan pengaturan keamanan WSP

Untuk WSP, data dalam perjalanan dienkripsi menggunakan enkripsi TLS 1.2. Secara default, semua cipher berikut diizinkan untuk enkripsi, dan klien dan server menegosiasikan cipher mana yang akan digunakan:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

Untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk memodifikasi Mode Keamanan TLS dan menambahkan suite sandi baru atau memblokir suite sandi tertentu. Penjelasan rinci tentang pengaturan ini dan cipher suite yang didukung disediakan di kotak dialog Configure security settings Group Policy.

Untuk mengkonfigurasi pengaturan keamanan WSP

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda. Misalnya, `example.com`.
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

   > **Note**
   >
   > Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka Konfigurasi pengaturan keamanan.
10. Dalam kotak dialog Konfigurasi pengaturan keamanan, pilih Diaktifkan. Tambahkan cipher suite yang ingin Anda izinkan dan hapus cipher suite yang ingin Anda blokir. Untuk informasi

selengkapnya tentang setelan ini, lihat deskripsi yang disediakan di kotak dialog Konfigurasi pengaturan keamanan.

11. Pilih OK.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace, dan setelah Anda memulai ulang WorkSpace sesi. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
    - Untuk me-reboot WorkSpace, di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces.
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Konfigurasikan ekstensi untuk WSP

Secara default, dukungan untuk WorkSpaces ekstensi dinonaktifkan. Jika diperlukan, Anda dapat mengonfigurasi WorkSpace untuk menggunakan ekstensi dengan cara berikut:

- Server dan klien - Aktifkan ekstensi untuk server dan klien
- Hanya server - Aktifkan ekstensi hanya untuk server
- Hanya klien - Aktifkan ekstensi hanya untuk klien

Untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk mengonfigurasi penggunaan ekstensi.

Untuk mengkonfigurasi ekstensi untuk WSP

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang bergabung ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda. Misalnya, `example.com`
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *yourdomainname*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *yourdomainname*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Konfigurasi ekstensi.
10. Dalam kotak dialog Konfigurasi ekstensi, pilih Diaktifkan dan kemudian atur opsi dukungan yang diinginkan. Pilih Client Only, Server dan Client, atau Server saja.
11. Pilih OK.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah Anda memulai ulang WorkSpace sesi. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

    - Nyalakan ulang WorkSpace. Di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces.
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Aktifkan atau nonaktifkan pengalihan kartu pintar untuk WSP

Secara default, Amazon tidak WorkSpaces diaktifkan untuk mendukung penggunaan kartu pintar baik untuk otentikasi pra-sesi atau otentikasi dalam sesi. Otentikasi pra-sesi mengacu pada otentikasi kartu pintar yang dilakukan saat pengguna masuk ke kartu mereka. WorkSpaces Autentikasi dalam sesi mengacu pada autentikasi yang dilakukan setelah masuk.

Jika diperlukan, Anda dapat mengaktifkan otentikasi pra-sesi dan dalam sesi untuk Windows WorkSpaces dengan menggunakan pengaturan Kebijakan Grup. Autentikasi pra-sesi juga harus diaktifkan melalui pengaturan direktori AD Connector Anda dengan menggunakan tindakan EnableClientAuthentication API atau perintah. enable-client-authentication AWS CLI Untuk informasi selengkapnya, lihat Aktifkan autentikasi Kartu Pintar untuk AD Connector dalam Panduan Administrasi AWS Directory Service .

> **Note**
>
> Untuk mengaktifkan penggunaan kartu pintar dengan Windows WorkSpaces, diperlukan langkah-langkah tambahan. Untuk informasi selengkapnya, lihat Gunakan kartu pintar untuk autentikasi.

Untuk mengaktifkan atau menonaktifkan pengalihan kartu pintar untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

   > **Note**
   >
   > Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .
8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan/nonaktifkan pengalihan kartu pintar.
10. Di kotak dialog Aktifkan/nonaktifkan pengalihan kartu pintar, pilih Diaktifkan atau Dinonaktifkan.
11. Pilih OKE.

12. Perubahan pengaturan Kebijakan Grup akan berlaku setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).

Aktifkan atau nonaktifkan WebAuthn pengalihan (FIDO2) untuk WSP

Secara default, Amazon WorkSpaces memungkinkan penggunaan WebAuthn autentikator untuk otentikasi dalam sesi. Otentikasi dalam sesi mengacu pada WebAuthn otentikasi yang dilakukan setelah masuk dan diminta oleh aplikasi web yang berjalan dalam sesi.

Persyaratan

WebAuthn (FIDO2) pengalihan untuk WSP membutuhkan yang berikut:

- Agen host WSP versi 2.0.0.1425 atau lebih tinggi
- WorkSpaces klien:
  - Linux Ubuntu 22.04 2023.3 atau lebih tinggi
  - Windows 5.19.0 atau lebih tinggi
  - Klien Mac 5.19.0 atau lebih tinggi
- Browser web yang diinstal saat Anda WorkSpaces menjalankan Ekstensi WebAuthn Pengalihan Amazon DCV:
  - Google Chrome 116+
  - Microsoft Edge 116+

Mengaktifkan atau menonaktifkan pengalihan WebAuthn (FIDO2) untuk Windows WorkSpaces

Jika diperlukan, Anda dapat mengaktifkan atau menonaktifkan dukungan untuk otentikasi dalam sesi dengan WebAuthn autentikator untuk Windows WorkSpaces dengan menggunakan pengaturan Kebijakan Grup. Jika Anda mengaktifkan atau tidak mengonfigurasi pengaturan ini, WebAuthn pengalihan akan diaktifkan dan pengguna dapat menggunakan autentikator lokal di dalam remote. WorkSpace

Ketika fitur diaktifkan, semua WebAuthn permintaan dari browser dalam sesi diarahkan ke klien lokal. Pengguna dapat menggunakan Windows Hello atau perangkat keamanan yang terpasang secara lokal seperti YubiKey atau autentikator lain yang sesuai dengan FIDO2 untuk menyelesaikan proses otentikasi.

Untuk mengaktifkan atau menonaktifkan WebAuthn pengalihan (FIDO2) untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan/nonaktifkan WebAuthn pengalihan.
10. Dalam kotak dialog Aktifkan/nonaktifkan WebAuthn pengalihan, pilih Diaktifkan atau Dinonaktifkan.
11. Pilih OK.
12. Perubahan setelan Kebijakan Grup akan berlaku setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, reboot WorkSpace dengan membuka WorkSpaces konsol Amazon dan memilih WorkSpace. Kemudian, pilih Actions, Reboot WorkSpaces).

Menginstal Ekstensi Pengalihan Amazon DCV WebAuthn

Pengguna perlu menginstal Ekstensi WebAuthn Pengalihan Amazon DCV untuk digunakan WebAuthn setelah fitur diaktifkan dengan melakukan salah satu hal berikut:

- Pengguna Anda akan diminta untuk mengaktifkan ekstensi browser di browser mereka.

> **Note**
>
> Ini adalah prompt browser satu kali. Pengguna Anda akan mendapatkan notifikasi saat Anda memperbarui versi agen WSP ke 2.0.0.1425 atau lebih tinggi. Jika pengguna akhir Anda tidak memerlukan WebAuthn pengalihan, mereka hanya dapat menghapus ekstensi dari browser. Anda juga dapat memblokir prompt instalasi WebAuthn Redirection Extension menggunakan kebijakan GPO di bawah ini.

- Anda dapat memaksa menginstal ekstensi pengalihan untuk pengguna Anda menggunakan kebijakan GPO di bawah ini. Jika Anda mengaktifkan kebijakan GPO, ekstensi akan diinstal secara otomatis ketika pengguna Anda meluncurkan browser yang didukung dengan akses internet.
- Pengguna Anda dapat menginstal ekstensi secara manual dengan Pengaya Microsoft Edge atau Toko Web Chrome.

Kelola dan instal ekstensi browser menggunakan Kebijakan Grup

Anda dapat menginstal Ekstensi WebAuthn Pengalihan Amazon DCV menggunakan Kebijakan Grup, baik secara terpusat dari domain Anda untuk host sesi yang digabungkan ke domain Direktori Aktif (AD) atau menggunakan Editor Kebijakan Grup Lokal untuk setiap host sesi. Proses ini akan berubah tergantung pada browser yang Anda gunakan.

Untuk Microsoft Edge

1. Unduh dan instal templat administratif Microsoft Edge.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.
8. Pilih Konfigurasi Komputer, Template Administratif, Microsoft Edge, dan Ekstensi
9. Buka Konfigurasi pengaturan manajemen ekstensi dan atur ke Diaktifkan.

10. Di bawah Konfigurasi pengaturan manajemen ekstensi, masukkan yang berikut ini:

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. Pilih OK.
12. Perubahan setelan Kebijakan Grup akan berlaku setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, reboot WorkSpace dengan membuka WorkSpaces konsol Amazon dan memilih WorkSpace. Kemudian, pilih Actions, Reboot WorkSpaces).

> **Note**
>
> Anda dapat memblokir pemasangan ekstensi dengan menerapkan pengaturan manajemen konfigurasi berikut:
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

Untuk Google Chrome

1. Unduh dan instal templat administratif Google Chrome. Untuk informasi selengkapnya, lihat Menyetel kebijakan Browser Chrome di PC terkelola.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.
8. Pilih Konfigurasi Komputer, Template Administratif, Google Chrome, dan Ekstensi
9. Buka Konfigurasi pengaturan manajemen ekstensi dan atur ke Diaktifkan.
10. Di bawah Konfigurasi pengaturan manajemen ekstensi, masukkan yang berikut ini:

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. Pilih OK.
12. Perubahan setelan Kebijakan Grup akan berlaku setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, reboot WorkSpace dengan membuka WorkSpaces konsol Amazon dan memilih WorkSpace. Kemudian, pilih Actions, Reboot WorkSpaces).

> **Note**
>
> Anda dapat memblokir pemasangan ekstensi dengan menerapkan pengaturan manajemen konfigurasi berikut:
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

Aktifkan atau nonaktifkan sesi pemutusan hubungan pada kunci layar untuk WSP

Jika diperlukan, Anda dapat memutuskan WorkSpaces sesi pengguna saat layar kunci Windows terdeteksi. Untuk menyambung kembali dari WorkSpaces klien, pengguna dapat menggunakan kata sandi atau kartu pintar mereka untuk mengautentikasi diri mereka sendiri, tergantung pada jenis otentikasi yang telah diaktifkan untuk mereka. WorkSpaces

Pengaturan Kebijakan Grup ini dinonaktifkan secara default. Jika diperlukan, Anda dapat mengaktifkan pemutusan sesi saat layar kunci Windows terdeteksi untuk Windows WorkSpaces dengan menggunakan pengaturan Kebijakan Grup.

> **Note**
>
> - Pengaturan Kebijakan Grup ini berlaku untuk sesi yang diautentikasi kata sandi dan kartu pintar.

- Untuk mengaktifkan penggunaan kartu pintar dengan Windows WorkSpaces, diperlukan langkah-langkah tambahan. Untuk informasi selengkapnya, lihat Gunakan kartu pintar untuk autentikasi.

Untuk mengaktifkan atau menonaktifkan sesi pemutusan pada kunci layar untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan/nonaktifkan sesi pemutusan hubungan pada kunci layar.
10. Di kotak dialog Aktifkan/nonaktifkan sesi pemutusan hubungan pada kunci layar, pilih Diaktifkan atau Dinonaktifkan.
11. Pilih OKE.

12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

    - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Aktifkan atau nonaktifkan Indirect Display Driver (IDD) untuk WSP

Secara default, WorkSpaces mendukung menggunakan Indirect Display Driver (IDD). Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

Untuk mengaktifkan atau menonaktifkan Indirect Display Driver (IDD) untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon Elastic Compute Cloud yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc).
3. Perluas hutan (Hutan:FQDN).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka konteks dengan mengklik kanan menu, dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah direktori Microsoft AD AWS Terkelola, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih Unit `yourdomainname` Organisasi (OU) atau OU apa pun di bawah nama domain itu, buka konteksnya dengan mengklik kanan menu, dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang `yourdomainname` OU, lihat Apa yang Dibuat di Panduan Administrasi Layanan AWS Direktori.

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Aktifkan Driver Tampilan AWS Tidak Langsung.
10. Dalam kotak dialog Aktifkan Driver Tampilan AWS Tidak Langsung, pilih Diaktifkan atau Dinonaktifkan.
11. Pilih OK.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

    a. Reboot WorkSpace (di WorkSpaces konsol, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
    b. Dalam prompt perintah administratif, masukkang`pupdate /force`.

Konfigurasikan pengaturan tampilan untuk WSP

WorkSpaces memungkinkan Anda mengonfigurasi beberapa pengaturan tampilan yang berbeda, termasuk frame rate maksimum, kualitas gambar minimum, kualitas gambar maksimum, dan pengkodean YUV. Sesuaikan pengaturan ini berdasarkan kualitas gambar, daya tanggap, dan akurasi warna yang Anda butuhkan.

Secara default, nilai frame rate maksimum adalah 25. Nilai frame rate maksimum menentukan frame maksimum yang diizinkan per detik (fps). Nilai 0 berarti tidak ada batas.

Secara default, nilai kualitas gambar minimum adalah 30. Kualitas gambar minimum dapat dioptimalkan untuk responsif gambar terbaik, atau kualitas gambar terbaik. Untuk daya tanggap terbaik, kurangi kualitas minimum. Untuk kualitas terbaik, tingkatkan kualitas minimum.

- Nilai ideal untuk daya tanggap terbaik adalah antara 30 dan 90.
- Nilai ideal untuk kualitas terbaik adalah antara 60 dan 90.

Secara default, nilai kualitas gambar maksimum adalah 80. Kualitas gambar maksimum tidak memengaruhi respons atau kualitas gambar, tetapi menetapkan maksimum untuk membatasi penggunaan jaringan.

Secara default, pengkodean gambar diatur ke YUV420. Memilih Aktifkan pengkodean YUV444 memungkinkan pengkodean YUV444 untuk akurasi warna yang tinggi.

Untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk mengonfigurasi frame rate maksimum, kualitas gambar minimum, dan nilai kualitas gambar maksimum.

Untuk mengkonfigurasi pengaturan tampilan untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang bergabung ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).
4. Perluas Domain.
5. Perluas contoh FQDN.Atau Anda,. `example.com`
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

   > **Note**
   >
   > Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .
8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Konfigurasi pengaturan tampilan.
10. Dalam kotak dialog Konfigurasikan pengaturan tampilan, pilih Diaktifkan dan kemudian atur laju bingkai maksimum (fps), kualitas gambar minimum, dan nilai kualitas gambar maksimum ke level yang diinginkan.
11. Pilih OK.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah Anda memulai ulang WorkSpace sesi. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

- Reboot WorkSpace. WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces
- Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Mengaktifkan atau menonaktifkan VSync untuk AWS Virtual Display-Only Driver untuk WSP

Secara default, WorkSpaces mendukung penggunaan fitur vSync untuk AWS Virtual Display-Only Driver. Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

Untuk mengaktifkan atau menonaktifkan vSync untuk Windows WorkSpaces

1. Pastikan template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon Elastic Compute Cloud yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc).
3. Perluas hutan (Hutan:FQDN).
4. Perluas Domain.
5. Perluas FQDN Anda (misalnya, `example.com`).
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka konteks dengan mengklik kanan menu, dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah direktori Microsoft AD AWS Terkelola, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih Unit `yourdomainname` Organisasi (OU) atau OU apa pun di bawah nama domain itu, buka konteksnya dengan mengklik menu, dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang `yourdomainname` OU, lihat Apa yang dibuat di AWS Directory Service Administration Guide.

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka fitur Aktifkan vSync dari pengaturan AWS Virtual Display Only Driver.

10. Dalam fitur Aktifkan vSync pada kotak dialog AWS Virtual Display Only Driver, pilih Diaktifkan atau Dinonaktifkan.
11. Pilih OK.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan hal berikut:

    a. Mulai ulang WorkSpace dengan melakukan salah satu dari berikut ini:

        i. Opsi 1 — Di WorkSpaces konsol, pilih yang ingin WorkSpace Anda reboot. Kemudian, pilih Actions, Reboot WorkSpaces.

        ii. Opsi 2 — Dalam prompt perintah administratif, masukkan`gpupdate /force`.

    b. Sambungkan kembali ke untuk menerapkan pengaturan. WorkSpace

    c. Reboot Workspace lagi.

Konfigurasikan verbositas log untuk WSP

Secara default, tingkat verbositas log untuk WSP WorkSpaces diatur ke Info. Anda dapat mengatur level log ke tingkat verbositas mulai dari yang paling sedikit bertele-tele hingga yang paling bertele-tele, seperti yang dijelaskan di sini:

- Kesalahan — paling tidak bertele-tele
- Peringatan
- Info - default
- Debug - paling bertele-tele

Untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk mengonfigurasi tingkat verbositas log.

Untuk mengkonfigurasi tingkat verbositas log untuk Windows WorkSpaces

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru untuk WSP diinstal di Central Store pengontrol domain untuk WorkSpaces direktori Anda.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
3. Perluas forest (Forest:***FQDN***).

4. Perluas Domain.
5. Perluas FQDN Anda. Misalnya, `example.com`.
6. Perluas Objek Kebijakan Grup.
7. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebagai gantinya, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini. Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Amazon, dan WSP.
9. Buka pengaturan Configure log verbosity.
10. Dalam kotak dialog Konfigurasi verbositas log, pilih Diaktifkan dan kemudian atur tingkat verbositas log ke debug, kesalahan, info, atau peringatan.
11. Pilih OK.
12. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah Anda memulai ulang WorkSpace sesi. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
    - Nyalakan ulang WorkSpace. Di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces.
    - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Instal templat administratif Kebijakan Grup untuk PCoIP

Untuk menggunakan pengaturan Kebijakan Grup yang khusus untuk Amazon WorkSpaces saat menggunakan protokol PCoIP, Anda harus menambahkan templat administratif Kebijakan Grup yang sesuai dengan versi agen PCoIP (baik 32-bit atau 64-bit) yang sedang digunakan untuk Anda. WorkSpaces

> **Note**
>
> Jika Anda memiliki campuran WorkSpaces dengan agen 32-bit dan 64-bit, Anda dapat menggunakan templat administratif Kebijakan Grup untuk agen 32-bit, dan pengaturan Kebijakan Grup Anda akan diterapkan ke agen 32-bit dan 64-bit. Ketika semua WorkSpaces Anda menggunakan agen 64-bit, Anda dapat beralih menggunakan template administratif untuk agen 64-bit.

Untuk menentukan apakah Anda WorkSpaces memiliki agen 32-bit atau agen 64-bit

1. Masuk ke WorkSpace, lalu buka Task Manager dengan memilih View, Send Ctrl+Alt+Delete atau dengan mengklik kanan task bar dan memilih Task Manager.
2. Dalam Manajer Tugas, buka tab Detail, klik kanan header kolom, dan pilih Pilih Kolom.
3. Di kotak dialog Pilih Kolom, pilih Platform, lalu pilih OKE.
4. Di tab Detail, temukan `pcoip_agent.exe`, lalu periksa nilainya di kolom Platform untuk menentukan bahwa agen PCoIP tersebut 32-bit atau 64-bit. (Anda mungkin melihat campuran WorkSpaces komponen 32-bit dan 64-bit; ini normal.)

Instal templat administratif Kebijakan Grup untuk PCoIP (32-bit)

Untuk menggunakan pengaturan Kebijakan Grup yang khusus untuk WorkSpaces saat menggunakan protokol PCoIP dengan agen PCoIP 32-bit, Anda harus menginstal template administratif Kebijakan Grup untuk PCoIP. Lakukan prosedur berikut pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke direktori Anda.

Untuk informasi selengkapnya tentang bekerja dengan file .adm, lihat Rekomendasi untuk mengelola file templat administratif Kebijakan Grup (.adm) dalam dokumentasi Microsoft.

Untuk menginstal templat administratif Kebijakan Grup untuk PCoIP

1. Dari Windows yang sedang berjalan WorkSpace, buat salinan `pcoip.adm` file di `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` direktori.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke unit organisasi di domain Anda yang berisi akun WorkSpaces mesin Anda.

3. Buka menu konteks (klik kanan) untuk unit organisasi akun mesin dan pilih Buat GPO di domain ini, dan tautkan di sini.
4. Di kotak dialog GPO Baru, masukkan nama deskriptif untuk GPO, seperti Kebijakan WorkSpaces Mesin, dan biarkan GPO Pemula Sumber disetel ke (tidak ada). Pilih OKE.
5. Buka menu konteks (klik kanan) untuk GPO baru dan pilih Edit.
6. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, dan Templat Administratif. Pilih Tindakan, Tambah/Hapus Templat dari menu utama.
7. Di kotak dialog Tambah/Hapus Templat, pilih Tambahkan, pilih file `pcoip.adm` yang disalin sebelumnya, lalu pilih Buka, Tutup.
8. Tutup Editor Manajemen Kebijakan Grup. Anda sekarang dapat menggunakan GPO ini untuk memodifikasi pengaturan Kebijakan Grup yang khusus untuk WorkSpaces.

Untuk memverifikasi bahwa file templat administratif diinstal dengan benar

1. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang bergabung ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan navigasikan ke dan pilih WorkSpaces GPO untuk akun mesin Anda WorkSpaces . Pilih Tindakan, Edit di menu utama.
2. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, Templat Administratif Klasik, dan Variabel Sesi PCoIP.
3. Anda sekarang dapat menggunakan objek Kebijakan Grup Variabel Sesi PCoIP ini untuk mengubah pengaturan Kebijakan Grup yang khusus untuk Amazon WorkSpaces saat menggunakan PCoIP.

> **Note**
>
> Untuk memungkinkan pengguna mengganti pengaturan Anda, pilih Pengaturan Administrator yang Dapat Diganti; jika tidak, pilih Pengaturan Administrator Tidak Dapat Diganti.

Instal templat administratif Kebijakan Grup untuk PCoIP (64-Bit)

Untuk menggunakan pengaturan Kebijakan Grup yang khusus untuk WorkSpaces saat menggunakan protokol PCoIP, Anda harus menambahkan template administratif Kebijakan Grup `PCoIP.admx` dan `PCoIP.adml` file untuk PCoIP ke Central Store pengontrol domain untuk

direktori Anda. WorkSpaces Untuk informasi selengkapnya tentang file `.admx` dan `.adml`, lihat Cara membuat dan mengelola Penyimpanan Pusat untuk Templat Administratif Kebijakan Grup di Windows.

Prosedur berikut menjelaskan cara membuat Penyimpanan Pusat dan menambahkan file templat administratif ke dalamnya. Lakukan prosedur berikut pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke direktori Anda WorkSpaces .

Untuk menginstal file templat administratif Kebijakan Grup untuk PCoIP

1. Dari Windows yang sedang berjalan WorkSpace, buat salinan `PCoIP.adml` file `PCoIP.admx` dan file di `C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions` direktori. File `PCoIP.adml` berada di dalam subfolder `en-US` dari direktori tersebut.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka Windows File Explorer, dan di bilah alamat, masukkan nama domain yang memenuhi syarat penuh (FQDN) organisasi Anda, seperti. `\\example.com`
3. Buka folder `sysvol`.
4. Buka folder dengan nama *`FQDN`*.
5. Buka folder `Policies`. Anda sekarang seharusnya berada di `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies`.
6. Jika belum ada, buat folder dengan nama `PolicyDefinitions`.
7. Buka folder `PolicyDefinitions`.
8. Salin file `PCoIP.admx` ke dalam folder `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions`.
9. Buat folder dengan nama `en-US` di dalam folder `PolicyDefinitions`.
10. Buka folder `en-US`.
11. Salin file `PCoIP.adml` ke dalam folder `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions\en-US`.

Untuk memverifikasi bahwa file templat administratif diinstal dengan benar

1. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
2. Perluas forest (Forest:***FQDN***).

3. Perluas Domain.
4. Perluas FQDN Anda (misalnya, `example.com`).
5. Perluas Objek Kebijakan Grup.
6. Pilih Kebijakan Domain Default, buka menu konteks (klik kanan), dan pilih Edit.

> **Note**
>
> Jika domain yang mendukung WorkSpaces adalah AWS Managed Microsoft AD direktori, Anda tidak dapat menggunakan Kebijakan Domain Default untuk membuat GPO Anda. Sebaliknya, Anda harus membuat dan menautkan GPO di bawah kontainer domain yang memiliki hak istimewa yang didelegasikan.
> Saat Anda membuat direktori dengan AWS Managed Microsoft AD, AWS Directory Service buat unit organisasi *`yourdomainname`* (OU) di bawah root domain. Nama OU ini didasarkan pada nama NetBIOS yang Anda ketik saat membuat direktori Anda. Jika Anda tidak menentukan nama NetBIOS, nama tersebut akan default ke bagian pertama dari nama DNS Direktori Anda (misalnya, dalam kasus `corp.example.com`, nama NetBIOS adalah `corp`).
> Untuk membuat GPO Anda, alih-alih memilih Kebijakan Domain Default, pilih OU (atau OU apa pun di bawahnya) *`yourdomainname`*, buka menu konteks (klik kanan), dan pilih Buat GPO di domain ini, dan Tautkan di sini.
> Untuk informasi selengkapnya tentang OU *`yourdomainname`*, lihat OU yang Dibuat dalam Panduan administrasi AWS Directory Service .

7. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Komputer, Kebijakan, Templat Administratif, dan Variabel Sesi PCoIP.
8. Anda sekarang dapat menggunakan objek Kebijakan Grup Variabel Sesi PCoIP ini untuk memodifikasi pengaturan Kebijakan Grup yang khusus untuk WorkSpaces saat menggunakan PCoIP.

> **Note**
>
> Untuk memungkinkan pengguna mengganti pengaturan Anda, pilih Pengaturan Administrator yang Dapat Diganti; jika tidak, pilih Pengaturan Administrator Tidak Dapat Diganti.

Mengelola pengaturan Kebijakan Grup untuk PCoIP

Gunakan pengaturan Kebijakan Grup untuk mengelola Windows Anda WorkSpaces yang menggunakan PCoIP.

Konfigurasikan dukungan printer untuk PCoIP

Secara default, WorkSpaces memungkinkan pencetakan jarak jauh Dasar, yang menawarkan kemampuan pencetakan terbatas karena menggunakan driver printer generik di sisi host untuk memastikan pencetakan yang kompatibel.

Pencetakan jarak jauh lanjutan untuk klien Windows memungkinkan Anda menggunakan fitur tertentu dari printer Anda, seperti pencetakan dua sisi, namun memerlukan instalasi driver printer yang cocok di sisi host.

Pencetakan jarak jauh diimplementasikan sebagai saluran virtual. Jika saluran virtual dinonaktifkan, pencetakan jarak jauh tidak berfungsi.

Untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk mengonfigurasi dukungan printer sesuai kebutuhan.

Untuk mengonfigurasi dukungan printer

1. Pastikan Anda telah menginstal template administratif Kebijakan WorkSpaces Grup terbaru untuk PCoIP (32-Bit) atau templat administratif Kebijakan WorkSpaces Grup untuk PCoIP (64-Bit).
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke Variabel Sesi PCoIP.
3. Buka pengaturan Konfigurasikan pencetakan jarak jauh.
4. Di kotak dialog Konfigurasikan pencetakan jarak jauh, lakukan salah satu hal berikut:
   - Untuk mengaktifkan pencetakan jarak jauh Lanjutan, pilih Diaktifkan, lalu di bawah Opsi, Konfigurasikan pencetakan jarak jauh, pilih Pencetakan Dasar dan Lanjutan untuk client Windows. Untuk secara otomatis menggunakan printer default komputer client saat ini, pilih Atur printer default secara otomatis.
   - Untuk menonaktifkan pencetakan, pilih Diaktifkan, lalu di bawah Opsi, Konfigurasikan pencetakan jarak jauh, pilih Pencetakan dinonaktifkan.
5. Pilih OKE.

6. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

   - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
   - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Secara default, pengalihan otomatis printer lokal dinonaktifkan. Anda dapat menggunakan pengaturan Kebijakan Grup untuk mengaktifkan fitur ini sehingga printer lokal Anda disetel sebagai printer default setiap kali Anda terhubung ke printer Anda WorkSpace.

> **Note**
>
> Pengalihan printer lokal tidak tersedia untuk Amazon Linux WorkSpaces.

Untuk mengaktifkan pengalihan otomatis printer lokal

1. Pastikan Anda telah menginstal template administratif Kebijakan WorkSpaces Grup terbaru untuk PCoIP (32-Bit) atau templat administratif Kebijakan WorkSpaces Grup untuk PCoIP (64-Bit).
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke Variabel Sesi PCoIP.
3. Buka pengaturan Konfigurasikan pencetakan jarak jauh.
4. Pilih Diaktifkan, lalu di bawah Opsi, Konfigurasikan pencetakan jarak jauh, pilih salah satu hal berikut:

   - Pencetakan dasar dan lanjutan untuk klien Windows
   - Pencetakan dasar
5. Pilih Set printer default secara otomatis, lalu pilih OKE.
6. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

- Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
- Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Aktifkan atau Nonaktifkan pengalihan clipboard untuk PCoIP

Secara default, WorkSpaces mendukung pengalihan clipboard. Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

Untuk mengaktifkan atau menonaktifkan pengalihan clipboard

1. Pastikan Anda telah menginstal template administratif Kebijakan WorkSpaces Grup terbaru untuk PCoIP (32-Bit) atau templat administratif Kebijakan WorkSpaces Grup untuk PCoIP (64-Bit).
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke Variabel Sesi PCoIP.
3. Buka pengaturan Konfigurasikan pengalihan clipboard.
4. Di Kotak dialog Konfigurasikan pengalihan clipboard, pilih Diaktifkan lalu pilih salah satu pengaturan berikut guna menentukan arah pengalihan clipboard yang diizinkan. Setelah selesai, pilih OKE.
   - Dinonaktifkan di kedua arah
   - Agen yang diaktifkan hanya untuk klien (WorkSpace ke komputer lokal)
   - Klien yang diaktifkan hanya untuk agen (komputer lokal ke WorkSpace)
   - Diaktifkan di kedua arah
5. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
   - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
   - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Pembatasan yang diketahui

Dengan pengalihan clipboard diaktifkan pada WorkSpace, jika Anda menyalin konten yang lebih besar dari 890 KB dari aplikasi Microsoft Office, aplikasi mungkin menjadi lambat atau tidak responsif hingga 5 detik.

Atur batas waktu melanjutkan sesi untuk PCoIP

Ketika Anda kehilangan konektivitas jaringan, sesi WorkSpaces klien aktif Anda terputus. WorkSpaces aplikasi klien untuk Windows dan macOS mencoba menghubungkan kembali sesi secara otomatis jika konektivitas jaringan dipulihkan dalam jangka waktu tertentu. Batas waktu resume sesi default adalah 20 menit, tetapi Anda dapat mengubah nilai WorkSpaces tersebut untuk yang dikendalikan oleh pengaturan Kebijakan Grup domain Anda.

Untuk mengatur nilai batas waktu melanjutkan sesi otomatis

1. Pastikan Anda telah menginstal template administratif Kebijakan WorkSpaces Grup terbaru untuk PCoIP (32-Bit) atau templat administratif Kebijakan WorkSpaces Grup untuk PCoIP (64-Bit).
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke Variabel Sesi PCoIP.
3. Buka pengaturan Konfigurasikan Kebijakan Menghubungkan Ulang Sesi secara Otomatis.
4. Di kotak dialog Konfigurasikan Kebijakan Menghubungkan Ulang Sesi secara Otomatis, pilih Diaktifkan, atur opsi Konfigurasikan Kebijakan Menghubungkan Ulang Sesi secara Otomatis ke batas waktu yang diinginkan, dalam hitungan menit, dan pilih OKE.
5. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
   - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
   - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Aktifkan atau nonaktifkan pengalihan audio-in untuk PCoIP

Secara default, Amazon WorkSpaces mendukung pengalihan data dari mikrofon lokal. Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

> **Note**
>
> Jika Anda memiliki setelan Kebijakan Grup yang membatasi logon lokal pengguna di dalamnya WorkSpaces, audio-in tidak akan berfungsi pada Anda. WorkSpaces Jika Anda menghapus setelan Kebijakan Grup itu, fitur audio-in diaktifkan setelah reboot berikutnya. WorkSpace Untuk informasi selengkapnya tentang pengaturan Kebijakan Grup ini, lihat Izinkan logon secara lokal dalam dokumentasi Microsoft.

Untuk mengaktifkan atau menonaktifkan pengalihan audio-in

1. Pastikan Anda telah menginstal template administratif Kebijakan WorkSpaces Grup terbaru untuk PCoIP (32-Bit) atau templat administratif Kebijakan WorkSpaces Grup untuk PCoIP (64-Bit).
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke Variabel Sesi PCoIP.
3. Buka pengaturan Aktifkan/nonaktifkan audio di sesi PCoIP.
4. Di kotak dialog Aktifkan/nonaktifkan audio di sesi PCoIP, pilih Diaktifkan atau Dinonaktifkan.
5. Pilih OKE.
6. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
   - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
   - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Nonaktifkan pengalihan zona waktu untuk PCoIP

Secara default, waktu dalam Workspace diatur untuk mencerminkan zona waktu klien yang digunakan untuk terhubung ke WorkSpace. Perilaku ini dikendalikan melalui pengalihan zona waktu. Anda mungkin ingin menonaktifkan arah zona waktu karena berbagai alasan:

- Perusahaan Anda ingin semua karyawan bekerja di zona waktu tertentu (bahkan jika beberapa karyawan berada di zona waktu yang lain).

- Anda telah menjadwalkan tugas dalam WorkSpace yang dimaksudkan untuk dijalankan pada waktu tertentu di zona waktu tertentu.
- Pengguna Anda yang sering bepergian ingin mempertahankan zona waktu mereka WorkSpaces dalam satu zona waktu untuk konsistensi dan preferensi pribadi.

Jika diperlukan untuk Windows WorkSpaces, Anda dapat menggunakan pengaturan Kebijakan Grup untuk menonaktifkan fitur ini.

Untuk menonaktifkan pengalihan zona waktu

1. Pastikan Anda telah menginstal template administratif Kebijakan WorkSpaces Grup terbaru untuk PCoIP (32-Bit) atau templat administratif Kebijakan WorkSpaces Grup untuk PCoIP (64-Bit).
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke Variabel Sesi PCoIP.
3. Buka pengaturan Konfigurasikan pengalihan zona waktu.
4. Di kotak dialog Konfigurasikan pengalihan zona waktu, pilih Dinonaktifkan.
5. Pilih OKE.
6. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
   - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
   - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.
7. Atur zona waktu untuk WorkSpaces ke zona waktu yang diinginkan.

Zona waktu sekarang statis dan tidak lagi mencerminkan zona waktu mesin klien. WorkSpaces

Konfigurasikan pengaturan keamanan PCoIP

Untuk PCoIP, data dalam perjalanan dienkripsi menggunakan enkripsi TLS 1.2 dan penandatanganan permintaan SigV4. Protokol PCoIP menggunakan lalu lintas UDP terenkripsi, dengan enkripsi AES, untuk piksel streaming. Hubungan streaming, menggunakan port 4172 (TCP dan UDP), dienkripsi dengan menggunakan cipher AES-128 dan AES-256, tetapi default enkripsi

adalah 128-bit. Anda dapat mengubah default ini ke 256-bit dengan menggunakan pengaturan Kebijakan Grup Konfigurasikan Pengaturan Keamanan PCoIP.

Anda juga dapat menggunakan pengaturan Kebijakan Grup ini untuk mengubah Mode Keamanan TLS dan memblokir rangkaian penyandian tertentu. Penjelasan detail tentang pengaturan ini dan rangkaian penyandian yang didukung disediakan di kotak dialog Kebijakan Grup Konfigurasikan Pengaturan Keamanan PCoIP.

Untuk mengonfigurasi pengaturan keamanan PCoIP

1. Pastikan Anda telah menginstal template administratif Kebijakan WorkSpaces Grup terbaru untuk PCoIP (32-Bit) atau templat administratif Kebijakan WorkSpaces Grup untuk PCoIP (64-Bit).
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke Variabel Sesi PCoIP.
3. Buka pengaturan Konfigurasikan Pengaturan Keamanan PCoIP.
4. Di kotak dialog Konfigurasikan Pengaturan Keamanan PCoIP, pilih Diaktifkan. Untuk mengatur enkripsi default untuk lalu lintas streaming ke 256-bit, buka opsi Cipher Enkripsi Data PCoIP, dan pilih Hanya AES-256-GCM.
5. (Opsional) Sesuaikan pengaturan Mode Keamanan TLS, lalu daftarkan rangkaian penyandian apa pun yang ingin Anda blokir. Untuk informasi selengkapnya tentang pengaturan ini, lihat deskripsi yang tersedia di kotak dialog Konfigurasikan Pengaturan Keamanan PCoIP.
6. Pilih OKE.
7. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
   - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
   - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Aktifkan pengalihan USB untuk YubiKey U2F

> **Note**

Amazon WorkSpaces saat ini mendukung pengalihan USB hanya untuk YubiKey U2F. Jenis perangkat USB lainnya mungkin dialihkan tetapi tidak didukung dan mungkin tidak berfungsi dengan baik.

Untuk mengaktifkan pengalihan USB untuk YubiKey U2F

1. Pastikan Anda telah menginstal template administratif Kebijakan WorkSpaces Grup terbaru untuk PCoIP (32-Bit) atau templat administratif Kebijakan WorkSpaces Grup untuk PCoIP (64-Bit).
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup (gpmc.msc) dan arahkan ke Variabel Sesi PCoIP.
3. Buka Aktifkan/nonaktifkan USB dalam pengaturan sesi PCOIP.
4. Pilih Diaktifkan, lalu pilih OK.
5. Buka pengaturan Konfigurasi PCoIP USB yang diizinkan dan aturan perangkat yang tidak diizinkan.
6. Pilih Diaktifkan, dan di bawah Masukkan tabel otorisasi USB (maksimum sepuluh aturan), konfigurasikan aturan daftar izin perangkat USB Anda.

   - Aturan otorisasi - 110500407. Nilai ini merupakan kombinasi dari Vendor ID (VID) dan Product ID (PID). Format untuk kombinasi VID/PID adalah 1xxxxyyyy, di mana xxxx adalah VID dalam format heksadesimal dan yyyy adalah PID dalam format heksadesimal. Untuk contoh ini, 1050 adalah VID, dan 0407 adalah PID. Untuk nilai YubiKey USB lainnya, lihat Nilai ID YubiKey USB.
7. Di bawah Masukkan tabel otorisasi USB (maksimum sepuluh aturan), konfigurasikan aturan daftar blok perangkat USB Anda.

   - Untuk Aturan Tidak Otorisasi, atur string kosong. Ini berarti bahwa hanya perangkat USB dalam daftar otorisasi yang diizinkan.

> **Note**
>
> Anda dapat menentukan maksimum 10 aturan otorisasi USB dan maksimum 10 aturan tidak otorisasi USB. Gunakan karakter vertical bar (|) untuk memisahkan beberapa

aturan. Untuk informasi rinci tentang aturan otorisasi/tidak otorisasi, lihat Teradici PCoIP Standard Agent untuk Windows.

8. Pilih OK.
9. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:
   - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
   - Dalam prompt perintah administratif, masukkan**`gpupdate /force`**.

Setelah pengaturan berlaku, semua perangkat USB yang didukung dapat mengarahkan ulang ke WorkSpaces kecuali pembatasan dikonfigurasi melalui pengaturan aturan perangkat USB.

Atur masa pakai maksimum untuk tiket Kerberos

Jika Anda belum menonaktifkan fitur Remember Me dari Windows Anda WorkSpaces, WorkSpace pengguna Anda dapat menggunakan kotak centang Remember Me atau Keep me login di aplikasi WorkSpaces klien mereka untuk menyimpan kredensialnya. Fitur ini memungkinkan pengguna untuk dengan mudah terhubung ke mereka WorkSpaces saat aplikasi klien tetap berjalan. Kredensial pengguna di-cache dengan aman hingga masa pakai maksimum tiket Kerberos mereka.

Jika Anda WorkSpace menggunakan direktori AD Connector, Anda dapat mengubah masa pakai tiket Kerberos maksimum untuk WorkSpaces pengguna Anda melalui Kebijakan Grup dengan mengikuti langkah-langkah dalam Masa Pakai Maksimum untuk Tiket Pengguna dalam dokumentasi Microsoft Windows.

Untuk mengaktifkan atau menonaktifkan fitur Ingatkan Saya, lihat Aktifkan kemampuan WorkSpace manajemen swalayan untuk pengguna Anda.

Konfigurasikan pengaturan server proksi perangkat untuk akses internet

Secara default, aplikasi WorkSpaces klien menggunakan server proxy yang ditentukan dalam pengaturan sistem operasi perangkat untuk lalu lintas HTTPS (port 443). Aplikasi WorkSpaces klien Amazon menggunakan port HTTPS untuk pembaruan, pendaftaran, dan otentikasi.

> **Note**
>
> Server proxy yang memerlukan otentikasi dengan kredenal masuk tidak didukung.

Anda dapat mengonfigurasi pengaturan server proxy perangkat untuk Windows Anda WorkSpaces melalui Kebijakan Grup dengan mengikuti langkah-langkah di Konfigurasikan proxy perangkat dan pengaturan konektivitas internet dalam dokumentasi Microsoft.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien WorkSpaces Windows, lihat Server Proxy di Panduan WorkSpaces Pengguna Amazon.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien WorkSpaces macOS, lihat Server Proxy di Panduan Pengguna WorkSpaces Amazon.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien Akses WorkSpaces Web, lihat Server Proxy di Panduan WorkSpaces Pengguna Amazon.

Proksi lalu lintas desktop

Untuk PCoIP WorkSpaces, aplikasi klien desktop tidak mendukung penggunaan server proxy atau dekripsi TLS dan inspeksi untuk lalu lintas port 4172 di UDP (untuk lalu lintas desktop). Mereka membutuhkan koneksi langsung ke port 4172.

Untuk WSP WorkSpaces, aplikasi klien WorkSpaces Windows (versi 5.1 ke atas) dan aplikasi klien macOS (versi 5.4 ke atas) mendukung penggunaan server proxy HTTP untuk lalu lintas TCP port 4195. Dekripsi dan inspeksi TLS tidak didukung.

WSP tidak mendukung penggunaan proxy untuk lalu lintas desktop melalui UDP. Hanya aplikasi klien desktop WorkSpaces Windows dan macOS dan akses web WSP yang mendukung penggunaan proxy, untuk lalu lintas TCP.

> **Note**
>
> Jika Anda memilih untuk menggunakan server proxy, panggilan API yang dibuat aplikasi klien ke WorkSpaces layanan juga diproksi. Panggilan API dan lalu lintas desktop harus melewati server proxy yang sama.

Rekomendasi tentang penggunaan server proxy

Kami tidak merekomendasikan penggunaan server proxy dengan lalu lintas WorkSpaces desktop Anda.

Lalu lintas WorkSpaces desktop Amazon sudah dienkripsi, jadi proxy tidak meningkatkan keamanan. Proxy mewakili lompatan tambahan di jalur jaringan yang dapat memengaruhi kualitas streaming dengan memperkenalkan latensi. Proxy juga berpotensi mengurangi throughput jika proxy tidak berukuran benar untuk menangani lalu lintas streaming desktop. Selain itu, sebagian besar proxy tidak dirancang untuk mendukung koneksi jangka panjang WebSocket (TCP) dan dapat memengaruhi kualitas dan stabilitas streaming.

Jika Anda harus menggunakan proxy, cari server proxy Anda sedekat mungkin dengan WorkSpace klien, sebaiknya di jaringan yang sama, untuk menghindari penambahan latensi jaringan, yang dapat berdampak negatif pada kualitas dan daya tanggap streaming.

Aktifkan Amazon WorkSpaces untuk dukungan Plugin Media Rapat Zoom

Pengguna dengan izin administrator ke Active Directory dapat menghasilkan kunci registri menggunakan Objek Kebijakan Grup (GPO) mereka. Ini memungkinkan pengguna untuk mengirim kunci registri ke semua Windows WorkSpaces dalam domain Anda menggunakan pembaruan paksa. Atau, pelanggan dengan hak admin juga dapat menginstal kunci registri satu per satu di WorkSpaces host mereka.

Prasyarat untuk menggunakan Zoom untuk WorkSpaces

Versi WorkSpaces klien yang didukung: Windows: 5.4.0.xxxx atau lebih tinggi.

Buat kunci registri pada WorkSpaces host Windows

Selesaikan prosedur berikut untuk membuat kunci registri pada WorkSpaces host Windows. Kunci registri diperlukan untuk menggunakan Zoom pada Windows WorkSpaces.

1. Buka Windows Registry Editor sebagai administrator.
2. Kunjungi `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`.
3. Jika tombol Extension tidak ada, klik kanan dan pilih New > Key dan beri nama Extension.
4. Di tombol Ekstensi baru, klik kanan dan pilih Baru> DWORD dan beri nama aktifkan. Nama harus dalam huruf kecil.
5. Klik DWORD baru dan ubah Nilai menjadi 1.

6. Reboot komputer untuk menyelesaikan proses.
7. Di WorkSpaces host Anda, unduh dan instal klien Zoom VDI terbaru. Pada WorkSpaces klien Anda (5.4 atau lebih tinggi), unduh dan instal plugin klien Zoom VDI terbaru untuk Amazon. WorkSpaces Untuk informasi selengkapnya, lihat rilis dan unduhan VDI di situs web dukungan Zoom.

Luncurkan Zoom untuk memulai panggilan video Anda.

Pemecahan Masalah

Selesaikan tindakan berikut untuk memecahkan masalah Zoom pada Windows. WorkSpaces

- Konfirmasikan bahwa aktivasi kunci registri dan diterapkan dengan benar.
- Kunjungi `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`. Anda harus melihat`wse_core_dll`.
- Pastikan bahwa versi pada host dan klien benar dan sama.

Jika Anda terus mengalami kesulitan, hubungi AWS Support menggunakan AWS Support Pusat.

Anda dapat menggunakan contoh berikut untuk menerapkan GPO sebagai administrator direktori Anda.

WSE.admL:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native GPO
 template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
```

```
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</string>
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
```

```
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

Kelola Amazon Linux Anda WorkSpaces

Seperti halnya Windows WorkSpaces, Amazon Linux WorkSpaces adalah domain yang bergabung, sehingga Anda dapat menggunakan Pengguna dan Grup Direktori Aktif untuk:

- Kelola Amazon Linux Anda WorkSpaces
- Menyediakan akses ke mereka WorkSpaces untuk pengguna

Karena instans Linux tidak mematuhi Kebijakan Grup, kami merekomendasikan Anda untuk menggunakan solusi manajemen konfigurasi untuk mendistribusikan dan menerapkan kebijakan. Misalnya, Anda dapat menggunakan AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise, atau Ansible.

> **Note**
>
> Pengalihan printer lokal tidak tersedia untuk Amazon Linux WorkSpaces.

Kontrol perilaku Protokol WorkSpaces Streaming (WSP) di Amazon Linux WorkSpaces

Perilaku WSP dikendalikan oleh pengaturan konfigurasi dalam `wsp.conf` file, yang terletak di `/etc/wsp/` direktori. Untuk men-deploy dan menerapkan perubahan kepada kebijakan, gunakan solusi

manajemen konfigurasi yang mendukung Amazon Linux. Setiap perubahan berlaku ketika agen dijalankan.

> **Note**
>
> - Jika Anda membuat perubahan yang salah atau tidak didukung pada `wsp.conf` file, perubahan kebijakan mungkin tidak diterapkan pada koneksi yang baru dibuat pada file Anda WorkSpace.
> - Amazon Linux WorkSpaces pada bundel WSP saat ini memiliki batasan berikut:
>   - Saat ini hanya tersedia di AWS GovCloud (AS-Barat) dan AWS GovCloud (AS-Timur).
>   - Video-in tidak didukung.
>   - Sesi pemutusan sambungan pada kunci layar tidak didukung.

Bagian berikut menjelaskan cara mengaktifkan atau menonaktifkan fitur tertentu.

Konfigurasikan pengalihan clipboard untuk WSP Amazon Linux WorkSpaces

Secara default, WorkSpaces mendukung pengalihan clipboard. Gunakan file konfigurasi WSP untuk mengkonfigurasi fitur ini, jika diperlukan. Pengaturan ini berlaku saat Anda memutuskan dan menyambungkan kembali file. WorkSpace

Untuk mengkonfigurasi pengalihan clipboard untuk WSP Amazon Linux WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. ```
   clipboard = X
   ```

   Nilai yang mungkin untuk *X* adalah:

   `enabled`— Pengalihan clipboard diaktifkan di kedua arah (default)

   `disabled`— Pengalihan clipboard dinonaktifkan di kedua arah
   ```

`paste-only`— Pengalihan clipboard diaktifkan tetapi hanya memungkinkan Anda untuk menyalin konten dari perangkat klien lokal dan menempelkannya ke desktop host jarak jauh

`copy-only`— Pengalihan clipboard diaktifkan tetapi hanya memungkinkan Anda untuk menyalin konten dari desktop host jarak jauh dan menempelkannya ke perangkat klien lokal

Mengaktifkan atau menonaktifkan pengalihan audio-in untuk WSP Amazon Linux WorkSpaces

Secara default, WorkSpaces mendukung pengalihan audio-in. Gunakan file konfigurasi WSP untuk menonaktifkan fitur ini, jika diperlukan. Pengaturan ini berlaku ketika Anda memutuskan sambungan dan menyambung kembali ke. WorkSpace

Untuk mengaktifkan atau menonaktifkan pengalihan audio-in untuk WSP Amazon Linux WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Tambahkan baris berikut ke akhir file.

   ```
   audio-in = X
   ```

   Nilai yang mungkin untuk *X* adalah:

   `enabled`— Pengalihan audio-in diaktifkan (default)

   `disabled`— Pengalihan audio-in dinonaktifkan

Mengaktifkan atau menonaktifkan pengalihan zona waktu untuk WSP Amazon Linux WorkSpaces

Secara default, waktu dalam Workspace diatur untuk mencerminkan zona waktu klien yang digunakan untuk terhubung ke WorkSpace. Perilaku ini dikendalikan melalui pengalihan zona waktu. Anda mungkin ingin mematikan arah zona waktu karena alasan seperti berikut:

- Perusahaan Anda ingin semua karyawan bekerja di zona waktu tertentu (bahkan jika beberapa karyawan berada di zona waktu yang lain).
- Anda telah menjadwalkan tugas dalam WorkSpace yang dimaksudkan untuk dijalankan pada waktu tertentu di zona waktu tertentu.
- Pengguna Anda yang sering bepergian ingin mempertahankan zona waktu mereka WorkSpaces dalam satu zona waktu untuk konsistensi dan preferensi pribadi.

Gunakan file konfigurasi WSP untuk mengkonfigurasi fitur ini, jika diperlukan. Pengaturan ini berlaku setelah Anda memutuskan dan menyambung kembali ke. WorkSpace

Untuk mengaktifkan atau menonaktifkan pengalihan zona waktu untuk WSP Amazon Linux WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
   ```

2. Tambahkan baris berikut ke akhir file.

   ```
   timezone_redirect= X
   ```

   Nilai yang mungkin untuk *X* adalah:

   diaktifkan - Pengalihan zona waktu diaktifkan (default)

   dinonaktifkan - Pengalihan zona waktu dinonaktifkan

Kontrol perilaku Agen PCoIP di Amazon Linux WorkSpaces

Perilaku Agen PCoIP dikendalikan oleh pengaturan konfigurasi di dalam file `pcoip-agent.conf`, yang terletak di direktori `/etc/pcoip-agent/`. Untuk men-deploy dan menerapkan perubahan kepada kebijakan, gunakan solusi manajemen konfigurasi yang mendukung Amazon Linux. Setiap perubahan berlaku ketika agen dijalankan. Memulai ulang agen akan mengakhiri hubungan terbuka dan memulai ulang pengelola jendela. Untuk menerapkan perubahan apa pun, kami sarankan untuk me-reboot file. WorkSpace

> **Note**
>
> Jika Anda membuat perubahan yang salah atau tidak didukung pada `pcoip-agent.conf` file, Anda dapat WorkSpace menyebabkan Anda berhenti bekerja. Jika Anda WorkSpace berhenti bekerja, Anda mungkin perlu terhubung ke SSH WorkSpace menggunakan Anda untuk memutar kembali perubahan, atau Anda mungkin harus membangun kembali. WorkSpace

Bagian berikut menjelaskan cara mengaktifkan atau menonaktifkan fitur tertentu. Untuk daftar lengkap pengaturan yang tersedia, jalankan `man pcoip-agent.conf` dari terminal di Amazon Linux mana pun WorkSpace.

Konfigurasikan pengalihan clipboard untuk PCoIP Amazon Linux WorkSpaces

Secara default, WorkSpaces mendukung pengalihan clipboard. Gunakan konfigurasi Agen PCoIP untuk menonaktifkan fitur ini, jika diperlukan. Pengaturan ini berlaku saat Anda me-reboot file WorkSpace.

Untuk mengkonfigurasi pengalihan clipboard untuk PCoIP Amazon Linux WorkSpaces

1. Buka file `pcoip-agent.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Tambahkan baris berikut ke akhir file.

   ```
   pcoip.server_clipboard_state = X
   ```

   Nilai yang mungkin untuk *X* adalah:

   0 - Pengalihan clipboard dinonaktifkan di kedua arah

   1 - Pengalihan clipboard diaktifkan di kedua arah

   2 - Pengalihan Clipboard diaktifkan klien ke agen saja (izinkan salin dan tempel hanya dari perangkat klien lokal ke desktop host jarak jauh)

3 - Pengalihan Clipboard diaktifkan agen ke klien saja (izinkan salin dan tempel hanya dari desktop host jarak jauh ke perangkat klien lokal)

> **Note**
>
> Pengalihan clipboard diimplementasikan sebagai saluran virtual. Jika saluran virtual dinonaktifkan, pengalihan clipboard tidak bekerja. Untuk mengaktifkan saluran virtual, lihat Saluran Virtual PCoIP dalam dokumentasi Teradici.

Mengaktifkan atau menonaktifkan pengalihan audio-in untuk PCoIP Amazon Linux WorkSpaces

Secara default, WorkSpaces mendukung pengalihan audio-in. Gunakan konfigurasi Agen PCoIP untuk menonaktifkan fitur ini, jika diperlukan. Pengaturan ini berlaku saat Anda me-reboot file WorkSpace.

Untuk mengaktifkan atau menonaktifkan pengalihan audio masuk untuk PCoIP Amazon Linux WorkSpaces

1. Buka file `pcoip-agent.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Tambahkan baris berikut ke akhir file.

   ```
   pcoip.enable_audio = X
   ```

   Nilai yang mungkin untuk *X* adalah:

   0 - Pengalihan audio-in dinonaktifkan

   1 - Pengalihan audio-in diaktifkan

Mengaktifkan atau menonaktifkan pengalihan zona waktu untuk PCoIP Amazon Linux WorkSpaces

Secara default, waktu dalam Workspace diatur untuk mencerminkan zona waktu klien yang digunakan untuk terhubung ke WorkSpace. Perilaku ini dikendalikan melalui pengalihan zona waktu. Anda mungkin ingin mematikan arah zona waktu karena alasan seperti berikut:

- Perusahaan Anda ingin semua karyawan bekerja di zona waktu tertentu (bahkan jika beberapa karyawan berada di zona waktu yang lain).
- Anda telah menjadwalkan tugas dalam WorkSpace yang dimaksudkan untuk dijalankan pada waktu tertentu di zona waktu tertentu.
- Pengguna Anda yang sering bepergian ingin mempertahankan zona waktu mereka WorkSpaces dalam satu zona waktu untuk konsistensi dan preferensi pribadi.

Jika diperlukan untuk Linux WorkSpaces, Anda dapat menggunakan conf Agen PCoIP untuk menonaktifkan fitur ini. Pengaturan ini berlaku saat Anda me-reboot file WorkSpace.

Untuk mengaktifkan atau menonaktifkan pengalihan zona waktu untuk PCoIP Amazon Linux WorkSpaces

1. Buka file `pcoip-agent.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Tambahkan baris berikut ke akhir file.

   ```
   pcoip.enable_timezone_redirect= X
   ```

   Nilai yang mungkin untuk *X* adalah:

   0 - Pengalihan zona waktu dinonaktifkan

   1 - Pengalihan zona waktu diaktifkan

Berikan akses SSH ke administrator Amazon Linux WorkSpaces

Secara default, hanya pengguna dan akun yang ditetapkan dalam grup Admin Domain yang dapat terhubung ke Amazon Linux WorkSpaces dengan menggunakan SSH.

Kami menyarankan Anda membuat grup administrator khusus untuk administrator Amazon Linux Anda di Active WorkSpaces Directory.

Untuk mengaktifkan akses sudo untuk anggota grup Direktori Aktif Linux_Workspaces_Admins

1. Edit file `sudoers` dengan menggunakan `visudo`, seperti yang ditunjukkan pada contoh berikut.

```
[example\username@workspace-id ~]$ sudo visudo
```

2. Tambahkan baris berikut.

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Setelah Anda membuat grup administrator khusus, ikuti langkah-langkah ini guna mengaktifkan login untuk anggota grup.

Untuk mengaktifkan login untuk anggota grup Direktori Aktif Linux_ WorkSpaces _Admins

1. Edit `/etc/security/access.conf` dengan hak yang lebih tinggi.

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Tambahkan baris berikut.

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

Untuk informasi selengkapnya tentang mengaktifkan hubungan SSH, lihat Aktifkan koneksi SSH untuk Linux Anda WorkSpaces.

Ganti shell default untuk Amazon Linux WorkSpaces

Untuk mengganti shell default untuk Linux WorkSpaces, kami sarankan Anda mengedit `~/.bashrc` file pengguna. Misalnya, untuk menggunakan `Z shell` sebagai ganti shell `Bash`, tambahkan baris berikut ke /home/*username*/`.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> Setelah melakukan perubahan ini, Anda harus me-reboot WorkSpace atau keluar dari WorkSpace (bukan hanya memutuskan sambungan) dan kemudian masuk kembali agar perubahan diterapkan.

Lindungi repositori kustom dari akses yang tidak sah

Untuk mengontrol akses ke repositori kustom Anda, sebaiknya gunakan fitur keamanan yang ada di dalam Amazon Virtual Private Cloud (Amazon VPC) daripada menggunakan kata sandi. Misalnya, gunakan daftar kontrol akses jaringan (ACL) dan grup keamanan. Untuk informasi selengkapnya tentang fitur ini, lihat Keamanan dalam Panduan Pengguna Amazon VPC.

Jika Anda harus menggunakan kata sandi untuk melindungi repositori Anda, pastikan untuk membuat file ketentuan repositori `yum` Anda seperti yang ditunjukkan dalam File Ketentuan Repositoridalam dokumentasi Fedora.

Gunakan repositori Perpustakaan Ekstra Amazon Linux

Dengan Amazon Linux, Anda dapat menggunakan Perpustakaan Ekstra untuk menginstal pembaruan aplikasi dan perangkat lunak pada instans Anda. Untuk informasi tentang penggunaan Perpustakaan Ekstra, lihat Perpustakaan Ekstra (Amazon Linux) dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.

> **Note**
>
> Jika Anda menggunakan repositori Amazon Linux, Amazon Linux Anda WorkSpaces harus memiliki akses internet, atau Anda harus mengonfigurasi titik akhir virtual private cloud (VPC) ke repositori ini dan ke repositori Amazon Linux utama. Untuk informasi selengkapnya, lihat Menyediakan akses internet dari Anda WorkSpace.

Gunakan kartu pintar untuk otentikasi di Linux WorkSpaces

Paket Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) memungkinkan penggunaan kartu pintar Common Access Card (CAC) dan Personal Identity Verification (PIV) untuk otentikasi. Untuk informasi selengkapnya, lihat Gunakan kartu pintar untuk autentikasi.

Konfigurasikan pengaturan server proksi perangkat untuk akses internet

Secara default, aplikasi WorkSpaces klien menggunakan server proxy yang ditentukan dalam pengaturan sistem operasi perangkat untuk lalu lintas HTTPS (port 443). Aplikasi WorkSpaces klien Amazon menggunakan port HTTPS untuk pembaruan, pendaftaran, dan otentikasi.

> **Note**
>
> Server proxy yang memerlukan otentikasi dengan kredensyal masuk tidak didukung.

Anda dapat mengonfigurasi pengaturan server proxy perangkat untuk Linux Anda WorkSpaces melalui Kebijakan Grup dengan mengikuti langkah-langkah di Konfigurasikan proxy perangkat dan pengaturan konektivitas internet dalam dokumentasi Microsoft.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien WorkSpaces Windows, lihat Server Proxy di Panduan WorkSpaces Pengguna Amazon.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien WorkSpaces macOS, lihat Server Proxy di Panduan Pengguna WorkSpaces Amazon.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien Akses WorkSpaces Web, lihat Server Proxy di Panduan WorkSpaces Pengguna Amazon.

Proksi lalu lintas desktop

Untuk PCoIP WorkSpaces, aplikasi klien desktop tidak mendukung penggunaan server proxy atau dekripsi TLS dan inspeksi untuk lalu lintas port 4172 di UDP (untuk lalu lintas desktop). Mereka membutuhkan koneksi langsung ke port 4172.

Untuk WSP WorkSpaces, aplikasi klien WorkSpaces Windows (versi 5.1 ke atas) dan aplikasi klien macOS (versi 5.4 ke atas) mendukung penggunaan server proxy HTTP untuk lalu lintas TCP port 4195. Dekripsi dan inspeksi TLS tidak didukung.

WSP tidak mendukung penggunaan proxy untuk lalu lintas desktop melalui UDP. Hanya aplikasi klien desktop WorkSpaces Windows dan macOS dan akses web WSP yang mendukung penggunaan proxy, untuk lalu lintas TCP.

> **Note**
>
> Jika Anda memilih untuk menggunakan server proxy, panggilan API yang dibuat aplikasi klien ke WorkSpaces layanan juga diproksi. Panggilan API dan lalu lintas desktop harus melewati server proxy yang sama.

Rekomendasi tentang penggunaan server proxy

Kami tidak merekomendasikan penggunaan server proxy dengan lalu lintas WorkSpaces desktop Anda.

Lalu lintas WorkSpaces desktop Amazon sudah dienkripsi, jadi proxy tidak meningkatkan keamanan. Proxy mewakili lompatan tambahan di jalur jaringan yang dapat memengaruhi kualitas streaming dengan memperkenalkan latensi. Proxy juga berpotensi mengurangi throughput jika proxy tidak berukuran benar untuk menangani lalu lintas streaming desktop. Selain itu, sebagian besar proxy tidak dirancang untuk mendukung koneksi jangka panjang WebSocket (TCP) dan dapat memengaruhi kualitas dan stabilitas streaming.

Jika Anda harus menggunakan proxy, cari server proxy Anda sedekat mungkin dengan WorkSpace klien, sebaiknya di jaringan yang sama, untuk menghindari penambahan latensi jaringan, yang dapat berdampak negatif pada kualitas dan daya tanggap streaming.

Kelola Ubuntu Anda WorkSpaces

Seperti halnya Windows dan Amazon Linux WorkSpaces, Ubuntu WorkSpaces adalah domain yang bergabung, sehingga Anda dapat menggunakan Pengguna dan Grup Direktori Aktif untuk:

- Kelola Ubuntu Anda WorkSpaces
- Menyediakan akses ke mereka WorkSpaces untuk pengguna

Anda dapat mengelola Ubuntu WorkSpaces dengan Kebijakan Grup dengan menggunakan AdSys. Lihat FAQ integrasi Direktori Aktif Ubuntu untuk informasi selengkapnya. Anda juga dapat menggunakan solusi konfigurasi dan manajemen lainnya, seperti Landscape dan Ansible.

Kontrol perilaku Protokol WorkSpaces Streaming (WSP) di Ubuntu WorkSpaces

Perilaku WSP dikendalikan oleh pengaturan konfigurasi dalam `wsp.conf` file, yang terletak di `/etc/wsp/` direktori. Untuk menerapkan dan menerapkan perubahan pada kebijakan, gunakan solusi manajemen konfigurasi yang mendukung Ubuntu. Setiap perubahan berlaku ketika agen dijalankan.

> **Note**
>
> Jika Anda membuat perubahan yang salah atau tidak didukung pada `wsp.conf` kebijakan mungkin tidak diterapkan pada koneksi yang baru dibuat ke Anda WorkSpace.

Bagian berikut menjelaskan cara mengaktifkan atau menonaktifkan fitur tertentu.

Mengaktifkan atau menonaktifkan pengalihan clipboard untuk Ubuntu WorkSpaces

Secara default, WorkSpaces mendukung pengalihan clipboard. Gunakan file konfigurasi WSP untuk menonaktifkan fitur ini, jika diperlukan.

Untuk mengaktifkan atau menonaktifkan pengalihan clipboard untuk Ubuntu WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Tambahkan baris berikut ke akhir `[policies]` grup.

   ```
   clipboard = X
   ```

   Nilai yang mungkin untuk *X* adalah:

   diaktifkan - Pengalihan Clipboard diaktifkan di kedua arah (default)

   dinonaktifkan - Pengalihan clipboard dinonaktifkan di kedua arah

   tempel saja - Pengalihan papan klip diaktifkan dan hanya memungkinkan Anda untuk menyalin konten dari perangkat klien lokal dan menempelkannya ke desktop host jarak jauh

salin saja - Pengalihan papan klip diaktifkan dan hanya memungkinkan Anda untuk menyalin konten dari desktop host jarak jauh dan menempelkannya ke perangkat klien lokal

Mengaktifkan atau menonaktifkan pengalihan audio-in untuk Ubuntu WorkSpaces

Secara default, WorkSpaces mendukung pengalihan audio-in. Gunakan file konfigurasi WSP untuk menonaktifkan fitur ini, jika diperlukan.

Untuk mengaktifkan atau menonaktifkan pengalihan audio-in untuk Ubuntu WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Tambahkan baris berikut ke akhir `[policies]` grup.

   ```
   audio-in = X
   ```

   Nilai yang mungkin untuk *X* adalah:

   diaktifkan - Pengalihan audio-in diaktifkan (default)

   dinonaktifkan - Pengalihan audio-in dinonaktifkan

Mengaktifkan atau menonaktifkan pengalihan video-in untuk Ubuntu WorkSpaces

Secara default, WorkSpaces mendukung pengalihan video-in. Gunakan file konfigurasi WSP untuk menonaktifkan fitur ini, jika diperlukan.

Untuk mengaktifkan atau menonaktifkan pengalihan video-in untuk Ubuntu WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Tambahkan baris berikut ke akhir `[policies]` grup.

```
video-in = X
```

Nilai yang mungkin untuk *X* adalah:

diaktifkan - Pengalihan video-in diaktifkan (default)

dinonaktifkan - Pengalihan video-in dinonaktifkan

Mengaktifkan atau menonaktifkan pengalihan zona waktu untuk Ubuntu WorkSpaces

Secara default, waktu dalam Workspace diatur untuk mencerminkan zona waktu klien yang digunakan untuk terhubung ke WorkSpace. Perilaku ini dikendalikan melalui pengalihan zona waktu. Anda mungkin ingin mematikan arah zona waktu karena alasan seperti berikut:

- Perusahaan Anda ingin semua karyawan bekerja di zona waktu tertentu (bahkan jika beberapa karyawan berada di zona waktu yang lain).
- Anda telah menjadwalkan tugas dalam WorkSpace yang dimaksudkan untuk dijalankan pada waktu tertentu di zona waktu tertentu.
- Pengguna Anda sering bepergian dan ingin tetap WorkSpaces berada dalam satu zona waktu untuk konsistensi dan preferensi pribadi.

Gunakan file konfigurasi WSP untuk mengkonfigurasi fitur ini, jika diperlukan.

Untuk mengaktifkan atau menonaktifkan pengalihan zona waktu untuk Ubuntu WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Tambahkan baris berikut ke akhir `[policies]` grup.

```
timezone-redirection = X
```

Nilai yang mungkin untuk *X* adalah:

diaktifkan - Pengalihan zona waktu diaktifkan (default)

dinonaktifkan - Pengalihan zona waktu dinonaktifkan

Mengaktifkan atau menonaktifkan pengalihan printer untuk Ubuntu WorkSpaces

Secara default, WorkSpaces mendukung pengalihan printer. Gunakan file konfigurasi WSP untuk menonaktifkan fitur ini, jika diperlukan.

Untuk mengaktifkan atau menonaktifkan pengalihan printer untuk Ubuntu WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Tambahkan baris berikut ke akhir `[policies]` grup.

   ```
   remote-printing = X
   ```

   Nilai yang mungkin untuk *X* adalah:

   diaktifkan - Pengalihan printer diaktifkan (default)

   dinonaktifkan - Pengalihan printer dinonaktifkan

Aktifkan atau nonaktifkan sesi pemutusan hubungan pada kunci layar untuk WSP

Aktifkan sesi pemutusan sambungan pada kunci layar untuk memungkinkan pengguna Anda mengakhiri WorkSpaces sesi mereka saat layar kunci Windows terdeteksi. Untuk menyambung kembali dari WorkSpaces klien, pengguna dapat menggunakan kata sandi atau kartu pintar mereka untuk mengautentikasi diri mereka sendiri, tergantung pada jenis otentikasi yang telah diaktifkan untuk mereka. WorkSpaces

Secara default, WorkSpaces tidak mendukung sesi pemutusan sambungan pada kunci layar. Gunakan file konfigurasi WSP untuk mengaktifkan fitur ini, jika diperlukan.

Untuk mengaktifkan atau menonaktifkan sesi pemutusan pada kunci layar untuk Windows WorkSpaces

1. Buka file `wsp.conf` di editor dengan hak yang lebih tinggi menggunakan perintah berikut.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Tambahkan baris berikut ke akhir `[policies]` grup.

```
disconnect-on-lock = X
```

   Nilai yang mungkin untuk *X* adalah:

   diaktifkan - Putuskan sambungan pada kunci layar diaktifkan

   dinonaktifkan - Putuskan sambungan pada kunci layar dinonaktifkan (default)

Berikan akses SSH ke administrator Ubuntu WorkSpaces

Secara default, hanya pengguna dan akun yang ditetapkan dalam grup Admin Domain yang dapat terhubung ke Ubuntu WorkSpaces dengan menggunakan SSH. Untuk mengaktifkan pengguna dan akun lain untuk terhubung ke Ubuntu WorkSpaces menggunakan SSH, kami sarankan Anda membuat grup administrator khusus untuk WorkSpaces administrator Ubuntu Anda di Active Directory.

Untuk mengaktifkan akses sudo bagi anggota grup **`Linux_WorkSpaces_Admins`** Active Directory

1. Edit file `sudoers` dengan menggunakan `visudo`, seperti yang ditunjukkan pada contoh berikut.

```
[username@workspace-id ~]$ sudo visudo
```

2. Tambahkan baris berikut.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Setelah Anda membuat grup administrator khusus, ikuti langkah-langkah ini guna mengaktifkan login untuk anggota grup.

Untuk mengaktifkan login untuk anggota grup **`Linux_WorkSpaces_Admins`** Active Directory

1. Edit/`etc/security/access.conf`dengan hak yang ditinggikan.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Tambahkan baris berikut.

```
+:(Linux_WorkSpaces_Admins):ALL
```

Dengan Ubuntu WorkSpaces Anda tidak perlu menambahkan nama domain saat menentukan nama pengguna untuk koneksi SSH, dan secara default, otentikasi kata sandi dinonaktifkan. Untuk terhubung melalui SSH, Anda perlu menambahkan kunci publik SSH Anda ke `$HOME/.ssh/authorized_keys` Ubuntu Anda WorkSpace, atau mengedit `/etc/ssh/sshd_config` untuk disetel PasswordAuthentication ke. `yes` Untuk informasi selengkapnya tentang mengaktifkan koneksi SSH, lihat Mengaktifkan koneksi SSH untuk Linux Anda. WorkSpaces

Ganti shell default untuk Ubuntu WorkSpaces

Untuk mengganti shell default untuk Ubuntu WorkSpaces, kami sarankan Anda mengedit `~/.bashrc` file pengguna. Misalnya, untuk menggunakan `Z shell` sebagai ganti shell `Bash`, tambahkan baris berikut ke `/home/username/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> Setelah melakukan perubahan ini, Anda harus me-reboot WorkSpace atau keluar dari WorkSpace (bukan hanya memutuskan sambungan) dan kemudian masuk kembali agar perubahan diterapkan.

Konfigurasikan pengaturan server proksi perangkat untuk akses internet

Secara default, aplikasi WorkSpaces klien menggunakan server proxy yang ditentukan dalam pengaturan sistem operasi perangkat untuk lalu lintas HTTPS (port 443). Aplikasi WorkSpaces klien Amazon menggunakan port HTTPS untuk pembaruan, pendaftaran, dan otentikasi.

> **Note**
>
> Server proxy yang memerlukan otentikasi dengan kredensyal masuk tidak didukung.

Anda dapat mengonfigurasi pengaturan server proxy perangkat untuk Ubuntu Anda WorkSpaces melalui Kebijakan Grup dengan mengikuti langkah-langkah di Konfigurasi proxy perangkat dan pengaturan konektivitas internet dalam dokumentasi Microsoft.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien WorkSpaces Windows, lihat Server Proxy di Panduan WorkSpaces Pengguna Amazon.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien WorkSpaces macOS, lihat Server Proxy di Panduan Pengguna WorkSpaces Amazon.

Untuk informasi selengkapnya tentang mengonfigurasi setelan proxy di aplikasi klien Akses WorkSpaces Web, lihat Server Proxy di Panduan WorkSpaces Pengguna Amazon.

Proksi lalu lintas desktop

Untuk PCoIP WorkSpaces, aplikasi klien desktop tidak mendukung penggunaan server proxy atau dekripsi TLS dan inspeksi untuk lalu lintas port 4172 di UDP (untuk lalu lintas desktop). Mereka membutuhkan koneksi langsung ke port 4172.

Untuk WSP WorkSpaces, aplikasi klien WorkSpaces Windows (versi 5.1 ke atas) dan aplikasi klien macOS (versi 5.4 ke atas) mendukung penggunaan server proxy HTTP untuk lalu lintas TCP port 4195. Dekripsi dan inspeksi TLS tidak didukung.

WSP tidak mendukung penggunaan proxy untuk lalu lintas desktop melalui UDP. Hanya aplikasi klien desktop WorkSpaces Windows dan macOS dan akses web WSP yang mendukung penggunaan proxy, untuk lalu lintas TCP.

> **Note**
>
> Jika Anda memilih untuk menggunakan server proxy, panggilan API yang dibuat aplikasi klien ke WorkSpaces layanan juga diproksi. Panggilan API dan lalu lintas desktop harus melewati server proxy yang sama.

Rekomendasi tentang penggunaan server proxy

Kami tidak merekomendasikan penggunaan server proxy dengan lalu lintas WorkSpaces desktop Anda.

Lalu lintas WorkSpaces desktop Amazon sudah dienkripsi, jadi proxy tidak meningkatkan keamanan. Proxy mewakili lompatan tambahan di jalur jaringan yang dapat memengaruhi kualitas streaming dengan memperkenalkan latensi. Proxy juga berpotensi mengurangi throughput jika proxy tidak berukuran benar untuk menangani lalu lintas streaming desktop. Selain itu, sebagian besar proxy tidak dirancang untuk mendukung koneksi jangka panjang WebSocket (TCP) dan dapat memengaruhi kualitas dan stabilitas streaming.

Jika Anda harus menggunakan proxy, cari server proxy Anda sedekat mungkin dengan WorkSpace klien, sebaiknya di jaringan yang sama, untuk menghindari penambahan latensi jaringan, yang dapat berdampak negatif pada kualitas dan daya tanggap streaming.

Optimalkan Amazon WorkSpaces untuk komunikasi waktu nyata

Amazon WorkSpaces menawarkan beragam teknik untuk memfasilitasi penyebaran aplikasi Unified Communication (UC) seperti Microsoft Teams, Zoom, Webex, dan lainnya. Dalam lanskap aplikasi kontemporer, sebagian besar aplikasi UC terdiri dari berbagai fitur, termasuk ruang obrolan 1:1, saluran obrolan grup kolaboratif, penyimpanan dan pertukaran file yang mulus, acara langsung, webinar, siaran, berbagi dan kontrol layar interaktif, papan tulis, dan kemampuan pesan audio/video offline. Sebagian besar fungsi ini tersedia dengan mulus WorkSpaces sebagai fitur standar, tanpa perlu penyetelan atau peningkatan tambahan. Namun, perlu dicatat bahwa elemen komunikasi real-time, terutama one-on-one panggilan dan pertemuan kelompok kolektif, merupakan pengecualian

untuk aturan ini. Keberhasilan penggabungan fungsionalitas tersebut sering menuntut fokus dan perencanaan khusus selama proses WorkSpaces penyebaran.

Saat merencanakan implementasi fungsi komunikasi real-time aplikasi UC di Amazon WorkSpaces, Anda memiliki tiga mode konfigurasi Real-Time Communication (RTC) yang berbeda untuk dipilih. Pilihannya tergantung pada aplikasi atau aplikasi spesifik yang ingin Anda berikan kepada pengguna Anda dan perangkat klien yang akan Anda gunakan.

Dokumen ini fokus pada pengoptimalan pengalaman pengguna untuk aplikasi UC paling umum di Amazon. WorkSpaces Untuk pengoptimalan spesifik WorkSpaces inti, silakan merujuk ke dokumentasi khusus mitra.

Topik

Ikhtisar mode pengoptimalan media

Berikut ini adalah opsi pengoptimalan media yang tersedia.

Opsi 1: Komunikasi Real-Time yang Dioptimalkan Media (Media Optimized RTC)

Dalam mode ini, aplikasi UC dan VoIP pihak ketiga dijalankan pada WorkSpace remote, sementara kerangka media mereka diturunkan ke klien yang didukung untuk komunikasi langsung. Aplikasi UC berikut menggunakan pendekatan ini di Amazon WorkSpaces:

- Pertemuan zoom
- Pertemuan Cisco Webex

Agar mode RTC Media Optimized berfungsi, vendor aplikasi UC harus mengembangkan integrasi dengan WorkSpaces menggunakan salah satu Kit Pengembangan Perangkat Lunak (SDK) yang tersedia, seperti SDK Ekstensi DCV. Mode ini membutuhkan komponen UC untuk diinstal pada perangkat klien.

Untuk informasi selengkapnya tentang mengonfigurasi mode ini, lihatKonfigurasikan RTC yang Dioptimalkan Media.

Opsi 2: Komunikasi Real-Time Dioptimalkan Dalam Sesi (RTC Dioptimalkan Dalam Sesi)

Dalam mode ini, aplikasi UC yang tidak berubah berjalan pada WorkSpace, menyalurkan lalu lintas audio dan video melalui Protokol WorkSpaces Streaming ke perangkat klien. Audio lokal dari mikrofon dan aliran video dari webcam diarahkan ke WorkSpace, di mana mereka dikonsumsi oleh aplikasi UC. Mode ini menyediakan kompatibilitas aplikasi yang luas dan secara efisien memberikan aplikasi UC dari remote WorkSpace ke berbagai platform klien. Anda tidak perlu menyebarkan komponen aplikasi UC ke perangkat klien.

Untuk informasi selengkapnya tentang mengonfigurasi mode ini, lihatKonfigurasikan RTC yang Dioptimalkan Dalam Sesi.

Opsi 3: Komunikasi Real-Time Langsung (RTC Langsung)

Dalam mode ini, aplikasi yang beroperasi di dalam WorkSpace mengambil kendali atas perangkat telepon fisik atau virtual yang terletak di meja pengguna atau OS klien. Ini menghasilkan lalu lintas audio yang melintasi langsung dari telepon fisik di workstation pengguna atau telepon virtual yang beroperasi pada perangkat klien ke rekan panggilan jarak jauh. Contoh penting dari aplikasi yang berfungsi dalam mode ini meliputi:

- Optimasi Amazon Connect untuk Amazon WorkSpaces
- Pembantu media WebRTC Genesys Cloud
- Microsoft Teams SIP Gateway
- Ponsel Microsoft Teams Desk dan tampilan Teams
- Partisipasi dalam konferensi audio melalui fitur dial-in atau “dial my phone” dari aplikasi UC.

Untuk informasi selengkapnya tentang mengonfigurasi mode ini, lihatKonfigurasikan RTC Langsung.

Mode optimasi RTC mana yang akan digunakan?

Mode optimasi RTC yang berbeda dapat digunakan secara bersamaan atau diatur untuk saling melengkapi sebagai fallback. Misalnya, pertimbangkan untuk mengaktifkan Media Optimized RTC untuk rapat Cisco Webex. Konfigurasi ini memastikan bahwa pengguna mengalami komunikasi yang dioptimalkan saat mengakses WorkSpace melalui klien desktop. Namun, dalam skenario di mana Webex diakses dari kios internet bersama yang tidak memiliki komponen pengoptimalan UC, Webex akan dengan mulus beralih ke mode RTC yang Dioptimalkan dalam sesi untuk mempertahankan

fungsionalitas. Ketika pengguna terlibat dengan beberapa aplikasi UC, mode konfigurasi RTC dapat bervariasi berdasarkan persyaratan unik mereka.

Tabel berikut mewakili fitur aplikasi UC umum dan mendefinisikan mode konfigurasi RTC mana yang memberikan hasil terbaik.

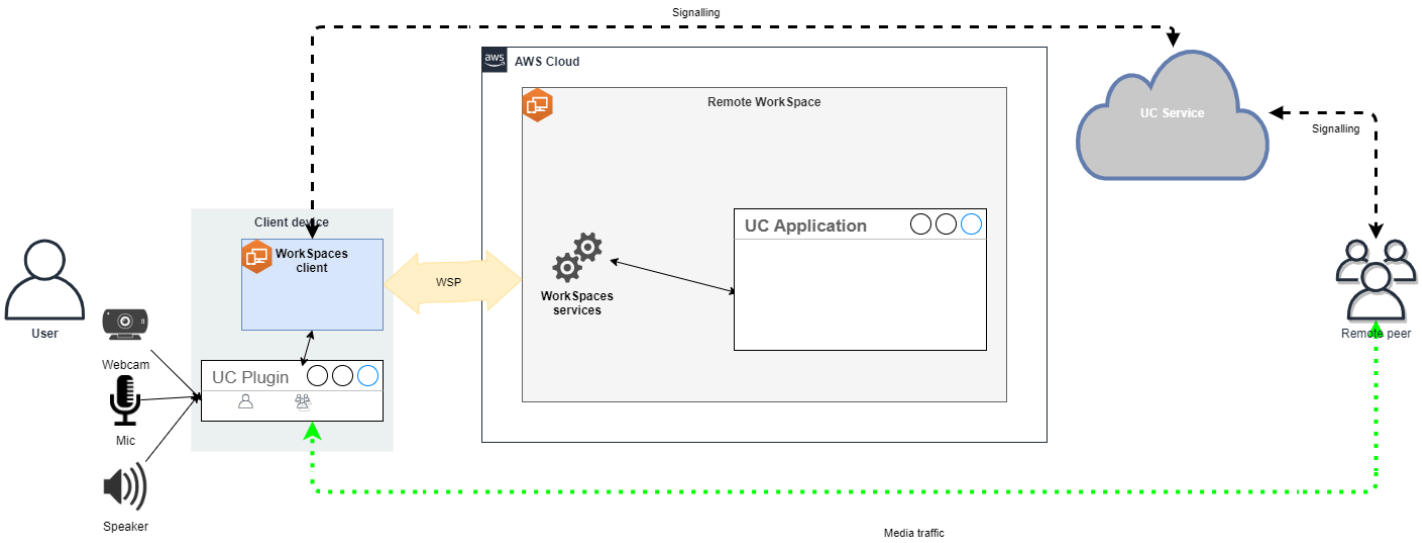
Fitur	RTC langsung	RTC yang Dioptimalkan Media	RTC yang Dioptimalkan Dalam Sesi
1:1 obrolan	Tidak memerlukan konfigurasi RTC		
Ruang obrolan grup	Tidak memerlukan konfigurasi RTC		
Konferensi audio grup	Terbaik	Terbaik	Baik
Konferensi video grup	Baik	Terbaik	Baik
Panggilan audio 1:1	Terbaik	Terbaik	Baik
Panggilan video 1:1	Baik	Terbaik	Baik
Papan tulis	Tidak memerlukan konfigurasi RTC		
Klip audio/video/pesan	Tidak berlaku	Baik	Terbaik
Berbagi File	Tidak berlaku	Tergantung pada aplikasi UC	Terbaik
Berbagi layar dan kontrol	Tidak berlaku	Tergantung pada aplikasi UC	Terbaik
Webinar/Acara siaran	Tidak berlaku	Baik	Terbaik

Panduan Optimasi RTC

Konfigurasikan RTC yang Dioptimalkan Media

Mode RTC Media Optimized dimungkinkan oleh vendor aplikasi UC menggunakan SDK yang disediakan oleh Amazon. Arsitektur membutuhkan vendor UC untuk mengembangkan plugin atau ekstensi khusus UC dan menyebarkannya ke klien.

SDK, yang mencakup opsi yang tersedia untuk umum seperti SDK Ekstensi DCV dan versi pribadi yang disesuaikan, menetapkan saluran kontrol antara modul aplikasi UC yang beroperasi di dalam WorkSpace dan plugin di sisi klien. Biasanya, saluran kontrol ini menginstruksikan ekstensi klien untuk memulai atau bergabung dengan panggilan. Setelah panggilan dibuat melalui ekstensi sisi klien, plugin UC menangkap audio dari mikrofon dan video dari webcam, yang kemudian ditransmisikan langsung ke cloud UC atau rekan panggilan. Audio yang masuk diputar secara lokal, dan video dilapis pada UI klien jarak jauh. Saluran kontrol bertanggung jawab untuk mengkomunikasikan status panggilan.



Amazon WorkSpaces saat ini mendukung aplikasi berikut dengan mode Media Optimized RTC:

- Pertemuan zoom (untuk PCoIP dan WSP) WorkSpaces
- Rapat Cisco Webex (hanya untuk WSP) WorkSpaces

Jika Anda menggunakan aplikasi yang tidak ada dalam daftar, disarankan untuk melibatkan vendor aplikasi dan meminta dukungan untuk WorkSpaces Media Optimized RTC. Untuk mempercepat proses ini, dorong mereka untuk menghubungi aws-av-offloading@amazon .com.

Sementara mode RTC Media Optimized meningkatkan kinerja panggilan dan meminimalkan pemanfaatan WorkSpace sumber daya, mode ini memiliki batasan tertentu:

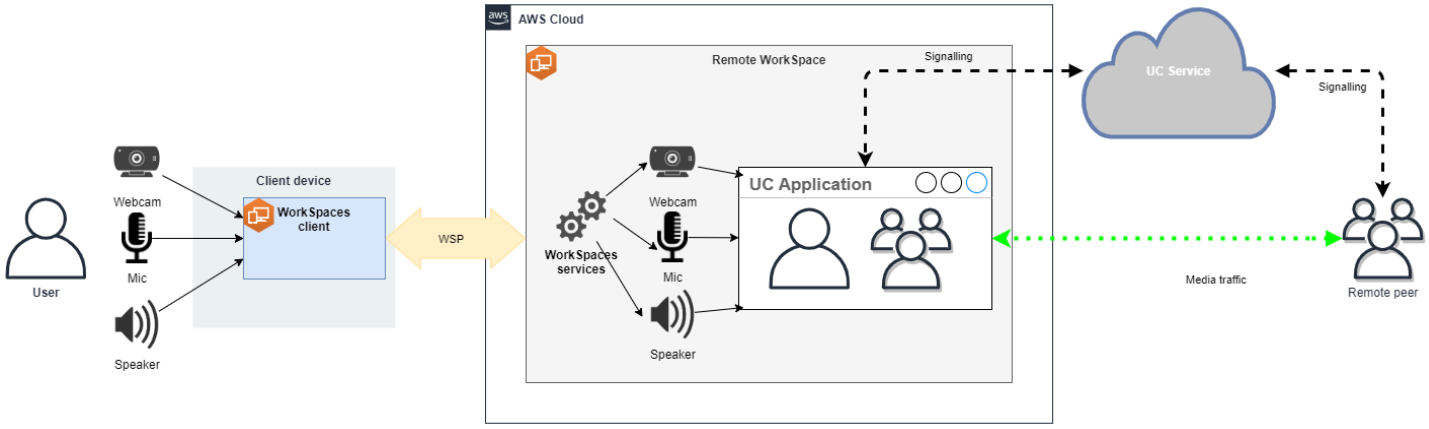
- Ekstensi klien UC harus diinstal pada perangkat klien.
- Ekstensi klien UC memerlukan manajemen dan pembaruan independen.
- Ekstensi klien UC mungkin tidak tersedia pada platform klien tertentu, seperti platform seluler, atau klien web.
- Beberapa fungsi aplikasi UC dapat dibatasi dalam mode ini; misalnya, perilaku berbagi layar mungkin berbeda.
- Penggunaan ekstensi sisi klien mungkin tidak cocok untuk skenario seperti Bring Your Own Device (BYOD) atau kios bersama.

Jika mode RTC Media Optimized terbukti tidak cocok untuk lingkungan Anda atau pengguna tertentu tidak dapat menginstal ekstensi klien, disarankan untuk mengonfigurasi mode RTC Dioptimalkan Dalam Sesi sebagai opsi mundur.

Konfigurasikan RTC yang Dioptimalkan Dalam Sesi

Dalam mode RTC Dioptimalkan Dalam Sesi, aplikasi UC beroperasi WorkSpace tanpa modifikasi apa pun, memberikan pengalaman seperti lokal. Streaming audio dan video yang dihasilkan oleh aplikasi ditangkap oleh WorkSpaces Streaming Protocol (WSP) dan ditransmisikan ke sisi klien. Pada klien, sinyal mikrofon (pada WSP dan PCoIP WorkSpaces) dan webcam (hanya pada WSP WorkSpaces) ditangkap, dialihkan kembali ke WorkSpace, dan diteruskan dengan mulus ke aplikasi UC.

Khususnya, opsi ini memastikan kompatibilitas yang luar biasa, bahkan dengan aplikasi lama, menawarkan pengalaman pengguna yang kohesif terlepas dari asal aplikasi. Optimasi dalam sesi bekerja dengan klien web juga.



WorkSpaces Streaming Protocol (WSP) telah dioptimalkan dengan cermat untuk meningkatkan kinerja mode RTC Jarak Jauh. Langkah-langkah pengoptimalan meliputi:

- Pemanfaatan transportasi QUIC berbasis UDP Adaptif, memastikan transmisi data yang efisien.
- Pembentukan jalur audio latensi rendah, memfasilitasi input dan output audio yang cepat.
- Implementasi codec audio yang dioptimalkan suara untuk menjaga kualitas audio sekaligus mengurangi pemanfaatan CPU dan jaringan.
- Pengalihan webcam, memungkinkan integrasi fungsi webcam.
- Konfigurasi resolusi webcam untuk mengoptimalkan kinerja.
- Integrasi codec tampilan adaptif untuk menyeimbangkan kecepatan dan kualitas visual.
- Koreksi jitter audio, menjamin transmisi audio yang lancar.

Pengoptimalan ini secara kolektif berkontribusi pada pengalaman yang kuat dan lancar dalam mode RTC Jarak Jauh.

Rekomendasi ukuran

Untuk mendukung mode RTC Jarak Jauh secara efektif, penting untuk memastikan ukuran Amazon yang tepat. WorkSpaces Remote WorkSpace harus memenuhi atau melampaui persyaratan sistem dari aplikasi Unified Communication (UC) masing-masing. Tabel berikut menguraikan WorkSpaces konfigurasi minimum yang didukung dan direkomendasikan untuk aplikasi UC populer saat digunakan untuk panggilan video dan audio:

			Panggilan video		Panggilan audio		
Aplikasi	Persyaratan CPU untuk aplikasi RTC	Persyaratan RAM untuk aplikasi RTC	Minimal didukung WorkSpace	Direkomendasikan WorkSpace	Minimal didukung WorkSpace	Direkomendasikan WorkSpace	Referensi
Tim Microsoft	Diperlukan 2 inti, 4 inti direkomendasikan	RAM 4.0 GB	Daya (4 vCPU, memori 16 GB)	PowerPro (8 vCPU, memori 32 GB)	Kinerja (2 vCPU, memori 8 GB)	Daya (4 vCPU, memori 16 GB)	Persyaratan perangkat keras untuk

			Panggilan video		Panggilan audio		
Aplikasi	Persyaratan CPU untuk aplikasi RTC	Persyaratan RAM untuk aplikasi RTC	Minimal didukung WorkSpace	Direkomendasikan WorkSpace	Minimal didukung WorkSpace	Direkomendasikan WorkSpace	Referensi
							Microsoft Teams
Perbesar	Diperlukan 2 inti, 4 inti direkomendasikan	RAM 4.0 GB	Daya (4 vCPU, memori 16 GB)	PowerPro (8 vCPU, memori 32 GB)	Kinerja (2 vCPU, memori 8 GB)	Daya (4 vCPU, memori 16 GB)	Persyaratan sistem zoom: Windows, macOS, Linux
Webex	Diperlukan 2 inti	RAM 4.0 GB	Daya (4 vCPU, memori 16 GB)	PowerPro (8 vCPU, memori 32 GB)	Kinerja (2 vCPU, memori 8 GB)	Daya (4 vCPU, memori 16 GB)	Persyaratan sistem untuk layanan Webex

Penting untuk dicatat bahwa konferensi video melibatkan penggunaan sumber daya yang signifikan untuk encoding dan decoding video. Dalam skenario mesin fisik, tugas-tugas ini diturunkan ke GPU. Dalam non-GPU WorkSpaces, tugas-tugas ini dilakukan pada CPU secara paralel dengan pengkodean protokol jarak jauh. Oleh karena itu, bagi pengguna yang secara teratur terlibat dalam streaming video atau panggilan video, memilih PowerPro konfigurasi sangat disarankan.

Berbagi layar juga mengkonsumsi sumber daya penting, dengan konsumsi sumber daya meningkat dengan resolusi yang lebih tinggi. Akibatnya, pada non-GPU WorkSpaces, berbagi layar seringkali terbatas pada frame rate yang lebih rendah.

Manfaatkan transportasi QUIC berbasis UDP dengan WorkSpaces Streaming Protocol (WSP)

Transportasi UDP sangat cocok untuk mentransmisikan aplikasi RTC. Untuk memaksimalkan efisiensi, pastikan jaringan Anda diatur untuk memanfaatkan transportasi QUIC untuk WSP. Perhatikan bahwa transportasi berbasis UDP hanya tersedia untuk klien asli.

Konfigurasikan aplikasi UC untuk WorkSpaces

Untuk kemampuan pemrosesan video yang ditingkatkan, seperti keburaman latar belakang, latar belakang virtual, reaksi, atau menyelenggarakan acara langsung, memilih GPU yang mendukung sangat WorkSpace penting untuk mencapai kinerja yang optimal.

Sebagian besar aplikasi UC memberikan panduan untuk menonaktifkan pemrosesan video canggih untuk mengurangi pemanfaatan CPU pada non-GPU. WorkSpaces

Untuk informasi lebih lanjut, lihat sumber daya berikut.

- Microsoft Teams: Tim untuk Infrastruktur Desktop Virtualisasi
- Zoom Meetings: Mengelola pengalaman pengguna untuk plugin VDI yang tidak kompatibel
- Webex: Panduan penerapan untuk Aplikasi Webex untuk Infrastruktur Desktop Virtual (VDI) - Kelola dan pecahkan masalah Aplikasi Webex untuk VDI [Aplikasi Webex]
- Google Meet: Menggunakan VDI

Aktifkan pengalihan audio dan webcam dua arah

Amazon WorkSpaces secara inheren mendukung audio-in, audio-out, dan pengalihan kamera melalui video-in secara default. Namun, jika fitur ini telah dinonaktifkan karena alasan tertentu, Anda dapat mengikuti panduan yang diberikan untuk mengaktifkan kembali pengalihan. Untuk informasi selengkapnya, lihat Aktifkan atau nonaktifkan pengalihan video untuk WSP di Panduan Administrasi Amazon. WorkSpaces Pengguna harus memilih kamera yang ingin mereka gunakan dalam sesi setelah menghubungkan. Untuk informasi selengkapnya, pengguna harus merujuk ke Webcam dan perangkat video lainnya di WorkSpaces Panduan Pengguna Amazon.

Batasi resolusi webcam maksimum

Untuk pengguna yang menggunakan Power atau PowerPro WorkSpaces untuk konferensi video, sangat disarankan untuk membatasi resolusi maksimum webcam yang dialihkan. Dalam hal ini PowerPro, resolusi maksimum yang disarankan adalah lebar 640 piksel dengan tinggi 480 piksel. Untuk Power, resolusi maksimum yang disarankan adalah lebar 320 piksel dengan tinggi 240 piksel.

Selesaikan langkah-langkah berikut untuk mengonfigurasi resolusi webcam maksimum.

1. Buka Windows Registry Editor.
2. Arahkan ke jalur registri berikut:

   ```
   HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
   ```

3. Buat nilai string bernama `max-resolution` dan atur ke resolusi yang diinginkan dalam `(X,Y)` format, di mana `X` mewakili jumlah piksel horizontal (lebar) dan `Y` mewakili jumlah piksel vertikal (tinggi). Misalnya, tentukan`(640,480)`) untuk mewakili resolusi dengan lebar 640 piksel dan tinggi 480 piksel.

Aktifkan konfigurasi audio yang dioptimalkan dengan suara

Secara default, WorkSpaces diatur untuk memberikan 7.1 audio dengan ketelitian tinggi dari klien, memastikan WorkSpaces kualitas pemutaran musik yang unggul. Namun, jika kasus penggunaan utama Anda melibatkan konferensi audio atau video, memodifikasi profil codec audio ke pengaturan yang dioptimalkan suara dapat menghemat sumber daya CPU dan jaringan.

Selesaikan langkah-langkah berikut untuk mengatur profil audio ke suara yang dioptimalkan.

1. Buka Windows Registry Editor.
2. Arahkan ke jalur registri berikut:

   ```
   HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
   ```

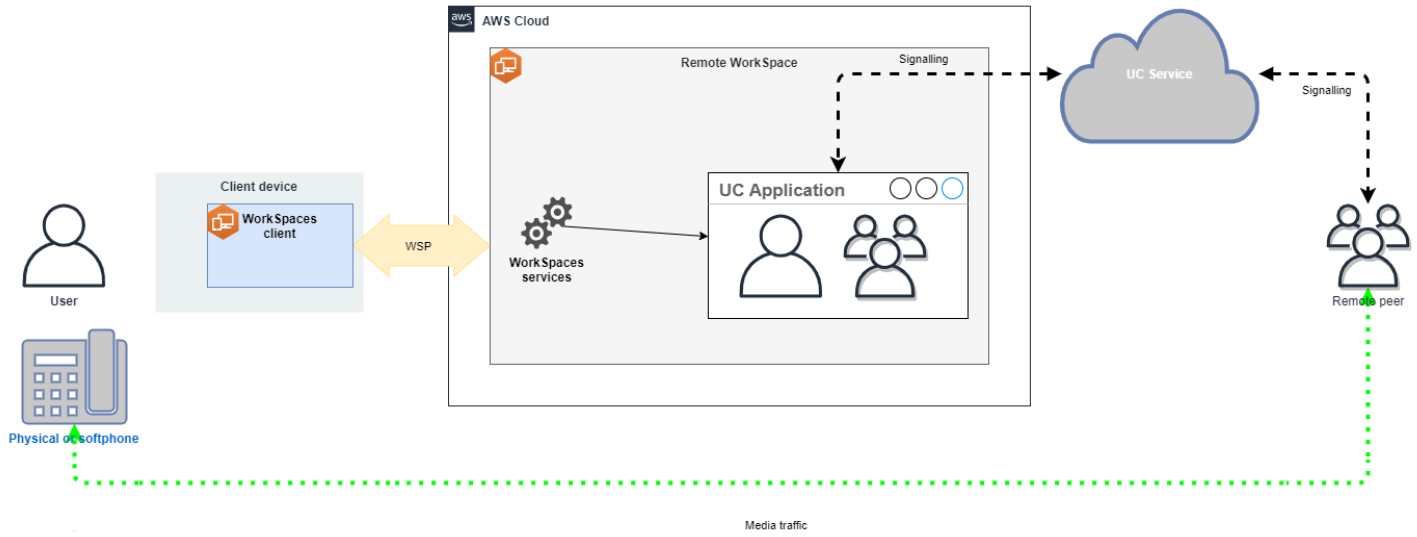
3. Buat nama nilai string `default-profile` dan atur `kevoice`.

Gunakan headset berkualitas baik untuk panggilan audio dan video

Untuk meningkatkan pengalaman audio dan mencegah gema, penting untuk menggunakan headset berkualitas tinggi. Memanfaatkan speaker desktop dapat menyebabkan masalah gema di ujung panggilan jarak jauh.

Konfigurasikan RTC Langsung

Konfigurasi mode Direct RTC tergantung pada aplikasi Unified Communication (UC) tertentu dan tidak memerlukan perubahan dalam konfigurasi. WorkSpaces Daftar berikut menawarkan kompilasi optimasi yang tidak lengkap untuk berbagai aplikasi UC.



- Tim Microsoft:
  - Rencana untuk SIP Gateway
  - Konferensi Audio di Microsoft 365
  - Rencanakan solusi suara Tim Anda
- Pertemuan Zoom:
  - Mengaktifkan atau menonaktifkan nomor dial-in panggilan tol
  - Menggunakan kontrol panggilan telepon meja
  - Mode pendamping telepon meja
- Webex:
  - Aplikasi Webex | Lakukan panggilan dengan telepon meja Anda
  - Aplikasi Webex | Opsi panggilan yang didukung
- BlueJeans:
  - Memanggil ke Rapat dari Telepon Meja
- Genesys:
  - Pembantu media WebRTC Genesys Cloud
- Amazon Connect:
  - Optimasi Amazon Connect untuk Amazon WorkSpaces
- Google Bertemu:
  - Menggunakan telepon untuk audio dalam rapat video

Kelola mode WorkSpace berjalan

Mode berjalan a WorkSpace menentukan ketersediaan langsungnya dan bagaimana Anda membayarnya (bulanan atau per jam). Anda dapat memilih antara mode berjalan berikut saat Anda membuat WorkSpace:

- AlwaysOn— Gunakan saat membayar biaya bulanan tetap untuk penggunaan Anda yang tidak terbatas WorkSpaces. Mode ini paling baik untuk pengguna yang menggunakan WorkSpace penuh waktu mereka sebagai desktop utama mereka.
- AutoStop— Gunakan saat membayar per jam Anda WorkSpaces . Dengan mode ini, Anda WorkSpaces berhenti setelah periode pemutusan tertentu, dan status aplikasi dan data disimpan.

Untuk informasi selengkapnya, lihat WorkSpaces Harga.

AutoStop WorkSpaces

Untuk mengatur waktu berhenti otomatis, pilih WorkSpace di WorkSpaces konsol Amazon, pilih Actions, Modify Running Mode Properties, dan kemudian atur AutoStop Waktu (jam). Secara default, AutoStop Waktu (jam) diatur ke 1 jam, yang berarti bahwa WorkSpace berhenti secara otomatis satu jam setelah WorkSpace terputus.

Setelah a WorkSpace terputus dan jangka AutoStop waktu telah kedaluwarsa, mungkin diperlukan beberapa menit tambahan untuk berhenti secara WorkSpace otomatis. Namun, penagihan berhenti segera setelah jangka AutoStop waktu berakhir, dan Anda tidak dikenakan biaya untuk waktu tambahan tersebut.

Jika memungkinkan, status desktop disimpan ke volume root file WorkSpace. WorkSpace Resume dilanjutkan ketika pengguna masuk, dan semua dokumen yang terbuka dan program yang berjalan kembali ke keadaan tersimpan.

AutoStop Graphics.g4dn, GraphicsPro .g4dn, Graphics, dan GraphicsPro WorkSpaces tidak mempertahankan status data dan program ketika mereka berhenti. Untuk Autostop ini WorkSpaces, kami sarankan untuk menyimpan pekerjaan Anda ketika Anda selesai menggunakannya setiap kali.

Untuk Bring Your Own License (BYOL) AutoStop WorkSpaces, sejumlah besar login bersamaan dapat mengakibatkan peningkatan waktu yang signifikan WorkSpaces untuk tersedia. Jika Anda mengharapkan banyak pengguna untuk masuk ke BYOL Anda AutoStop WorkSpaces pada saat yang sama, silakan berkonsultasi dengan manajer akun Anda untuk saran.

> **Important**
>
> AutoStop WorkSpaces berhenti secara otomatis hanya jika WorkSpaces terputus.

A WorkSpace terputus hanya dalam keadaan berikut:

- Jika pengguna secara manual memutuskan sambungan dari WorkSpace atau berhenti dari aplikasi WorkSpaces klien Amazon.
- Jika perangkat klien dimatikan.
- Jika tidak ada koneksi antara perangkat klien dan WorkSpace selama lebih dari 20 menit.

Sebagai praktik terbaik, AutoStop WorkSpace pengguna harus memutuskan sambungan secara manual dari mereka WorkSpaces ketika mereka selesai menggunakannya setiap hari. Untuk memutuskan sambungan secara manual, pilih Putuskan sambungan WorkSpace atau Keluar WorkSpaces dari Amazon WorkSpaces menu di aplikasi WorkSpaces klien untuk Linux, macOS, atau Windows. Untuk Android atau iPad, pilih Putuskan hubungan dari menu sidebar.

AutoStop WorkSpaces mungkin tidak berhenti secara otomatis dalam situasi berikut:

- Jika perangkat klien hanya terkunci, tidur, atau tidak aktif (misalnya, tutup laptop ditutup) alih-alih dimatikan, WorkSpaces aplikasi mungkin masih berjalan di latar belakang. Selama WorkSpaces aplikasi masih berjalan, WorkSpace mungkin tidak terputus, dan karena itu WorkSpace mungkin tidak berhenti secara otomatis.
- WorkSpaces dapat mendeteksi pemutusan hanya ketika pengguna menggunakan WorkSpaces klien. Jika pengguna menggunakan klien pihak ketiga, WorkSpaces mungkin tidak dapat mendeteksi pemutusan, dan oleh karena itu WorkSpaces mungkin tidak berhenti secara otomatis dan penagihan mungkin tidak ditangguhkan.

Mengubah mode berjalan

Anda dapat beralih di antara mode berjalan kapan saja.

Untuk memodifikasi mode berjalan dari a WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.

3. Pilih tombol WorkSpace untuk memodifikasi dan memilih Actions, Modify running mode.
4. Pilih mode berjalan baru, AlwaysOnatau AutoStop, lalu pilih Simpan.

Untuk memodifikasi mode berjalan WorkSpace menggunakan AWS CLI

Gunakan perintah modify-workspace-properties.

Berhenti dan mulai AutoStop WorkSpace

Ketika Anda AutoStop WorkSpaces terputus, mereka berhenti secara otomatis setelah periode pemutusan tertentu, dan penagihan per jam ditangguhkan. Untuk lebih mengoptimalkan biaya, Anda dapat secara manual menangguhkan biaya per jam yang terkait dengannya. AutoStop WorkSpaces WorkSpacePemberhentian dan semua aplikasi dan data disimpan untuk waktu berikutnya pengguna masuk ke file WorkSpace.

Ketika pengguna menyambung kembali ke stop WorkSpace, ia melanjutkan dari tempat yang ditinggalkannya, biasanya dalam waktu kurang dari 90 detik.

Anda dapat reboot (restart) AutoStop WorkSpaces yang tersedia atau dalam keadaan kesalahan.

Untuk menghentikan sebuah AutoStop WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih tombol WorkSpace untuk berhenti dan pilih Actions, Stop WorkSpaces.
4. Ketika diminta konfirmasi, pilih Berhenti WorkSpace.

Untuk memulai sebuah AutoStop WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih WorkSpaces untuk memulai dan pilih Tindakan, Mulai WorkSpaces.
4. Ketika diminta konfirmasi, pilih Mulai WorkSpace.

Untuk menghapus biaya infrastruktur tetap yang terkait AutoStop WorkSpaces, hapus WorkSpace dari akun Anda. Untuk informasi selengkapnya, lihat Menghapus WorkSpace.

Untuk berhenti dan mulai AutoStop WorkSpace menggunakan AWS CLI

Gunakan WorkSpaces perintah stop- WorkSpaces dan start-.

Mengelola aplikasi

Setelah Anda meluncurkan WorkSpace, Anda dapat melihat daftar semua bundel aplikasi yang terkait dengan Anda WorkSpace di WorkSpaces konsol.

Untuk melihat daftar semua bundel aplikasi yang terkait dengan WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Dari panel navigasi kiri, pilih WorkSpaces.
3. Pilih WorkSpace dan pilih Lihat Detail.
4. Di bawah Aplikasi, temukan daftar aplikasi yang terkait dengan ini WorkSpace, bersama dengan status pemasangannya.

Anda dapat memperbarui bundel aplikasi pada Anda dengan WorkSpace cara berikut:

- Instal bundel aplikasi di WorkSpace
- Copot pemasangan bundel aplikasi dari WorkSpace
- Instal bundel aplikasi dan hapus instalan kumpulan bundel aplikasi yang berbeda di WorkSpace

> **Note**
>
> - Untuk memperbarui bundel aplikasi, WorkSpace harus memiliki status `AVAILABLE` atau`STOPPED`.
> - Kelola aplikasi hanya tersedia untuk Windows WorkSpaces.
> - Kelola aplikasi hanya tersedia untuk bundel aplikasi yang berlangganan. AWS

Bundel yang didukung untuk Kelola aplikasi

Kelola aplikasi memungkinkan Anda menginstal dan menghapus instalan aplikasi berikut pada aplikasi Anda WorkSpaces. Untuk bundel Microsoft Office 2016 dan Microsoft Office 2019, Anda hanya dapat menghapus instalan.

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Standar LTSC Microsoft Office 2021
- Standar Microsoft Visio LTSC 2021
- Standar Proyek Microsoft 2021

Tabel berikut menunjukkan daftar kombinasi aplikasi dan sistem operasi yang didukung dan tidak didukung:

	Microsoft Office Professional Plus 2016 (32-bit)	Microsoft Office Professional Plus 2019 (64-bit)	Microsoft LTSC Office Professional Plus/ Standar 2021 (64-bit)	Microsoft Project Professional/Standar 2021 (64-bit)	Microsoft LTSC Visio Professional/Standar 2021 (64-bit)
Windows Server 2016	Hapus instalasi	Tidak didukung	Tidak didukung	Tidak didukung	Tidak didukung
Windows Server 2019	Tidak didukung	Hapus instalasi	Instal/copot pemasangan	Instal/copot pemasangan	Instal/copot pemasangan
Windows Server 2022	Tidak didukung	Hapus instalasi	Instal/copot pemasangan	Instal/copot pemasangan	Instal/copot pemasangan
Windows 10	Hapus instalasi	Hapus instalasi	Instal/copot pemasangan	Instal/copot pemasangan	Instal/copot pemasangan

	Microsoft Office Professional Plus 2016 (32-bit)	Microsoft Office Professional Plus 2019 (64-bit)	Microsoft LTSC Office Professional Plus/ Standar 2021 (64-bit)	Microsoft Project Professional/Standar 2021 (64-bit)	Microsoft LTSC Visio Professional/Standar 2021 (64-bit)
Windows 11	Hapus instalasi	Hapus instalasi	Instal/copot pemasangan	Instal/copot pemasangan	Instal/copot pemasangan

Important

- Aplikasi ini harus mengikuti edisi yang sama. Misalnya, Anda tidak dapat mencampur aplikasi Standar dengan aplikasi Profesional.
- Aplikasi ini harus mengikuti versi yang sama. Misalnya, Anda tidak dapat mencampur aplikasi 2019 dengan aplikasi 2021.
- Microsoft Office/Visio/Project 2021 Standard/Professional tidak didukung untuk Nilai, Grafik, dan bundel. GraphicsPro WorkSpaces
- Saat Anda menghapus bundel aplikasi Plus untuk Microsoft Office 2016 dari Anda WorkSpaces, Anda akan kehilangan akses ke solusi Trend Micro apa pun yang disertakan sebagai bagian dari WorkSpaces bundel Amazon itu. Jika Anda ingin terus menggunakan solusi Trend Micro dengan Amazon Anda WorkSpaces, Anda dapat membelinya secara terpisah di AWSpasar.
- Untuk menginstal/menghapus aplikasi Microsoft 365, Anda perlu membawa alat dan penginstal Anda sendiri, Kelola alur kerja aplikasi tidak dapat menginstal/menghapus aplikasi Microsoft 365.
- Anda tidak dapat membuat gambar kustom WorkSpaces dengan aplikasi yang diinstal melalui Kelola aplikasi tetapi Anda dapat membuat gambar khusus WorkSpaces dari mana Anda menghapus bundel aplikasi menggunakan Kelola aplikasi.
- Resolusi DNS harus diaktifkan untuk menggunakan Kelola aplikasi.

- Untuk wilayah opt-in, seperti Afrika (Cape Town), koneksi WorkSpaces internet harus diaktifkan pada tingkat direktori.

Untuk memperbarui bundel aplikasi pada WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih WorkSpace dan pilih Tindakan, Kelola aplikasi.
4. Di bawah Aplikasi saat ini Anda akan melihat daftar bundel aplikasi yang sudah diinstal pada ini WorkSpace dan di bawah Pilih aplikasi Anda memiliki daftar bundel aplikasi yang tersedia untuk diinstal pada ini. WorkSpace
5. Untuk menginstal bundel aplikasi pada ini WorkSpace:
   a. Pilih bundel aplikasi yang ingin Anda instal di sini WorkSpace, dan pilih Associate.
   b. Ulangi langkah sebelumnya untuk menginstal bundel aplikasi lainnya.
   c. Saat bundel aplikasi sedang diinstal, Anda akan melihatnya di bawah Aplikasi saat ini dengan `Pending install deployment` status.
6. Untuk menghapus bundel aplikasi dari ini: WorkSpace
   a. Di bawah Pilih aplikasi, pilih bundel aplikasi yang ingin Anda hapus dan pilih Disassociate.
   b. Ulangi langkah sebelumnya untuk menghapus bundel aplikasi lainnya.
   c. Saat bundel aplikasi dihapus, Anda akan melihatnya di bawah Aplikasi saat ini dengan status. `Pending uninstall deployment`
7. Untuk mengembalikan status instalasi atau instalasi bundel, lakukan salah satu hal berikut.
   - Jika Anda ingin mengembalikan bundel dari **`Pending uninstall deployment`** status, pilih aplikasi yang ingin Anda kembalikan, lalu pilih Associate.
   - Jika Anda ingin mengembalikan bundel dari **`Pending install deployment`** status, pilih aplikasi yang ingin Anda kembalikan, lalu pilih Disassociate.
8. Setelah bundel aplikasi yang Anda pilih untuk menginstal atau menghapus instalasi berada dalam status tertunda, pilih Menyebarkan aplikasi.

> **Important**
>
> Setelah Anda memilih Deploy aplikasi, sesi pengguna akhir akan berakhir dan tidak WorkSpaces akan dapat diakses saat aplikasi sedang diinstal atau dihapus.

9. Untuk mengonfirmasi tindakan Anda, ketik konfirmasi. Pilih paksa untuk menginstal atau menghapus bundel aplikasi yang berada dalam keadaan Kesalahan.
10. Untuk memantau kemajuan bundel aplikasi Anda:

    a. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.

    b. Di panel navigasi, pilih WorkSpaces. Anda dapat melihat status di bawah Status termasuk yang berikut ini.

    - MEMPERBARUI - Pembaruan bundel aplikasi masih berlangsung.
    - TERSEDIA/BERHENTI - Pembaruan bundel aplikasi selesai dan kembali ke keadaan semula. WorkSpace

    c. Untuk memantau status instalasi atau penghapusan instalasi bundel aplikasi Anda, pilih WorkSpace dan pilih Lihat Detail. Di bawah Aplikasi, Anda dapat melihat status di bawah Status, termasuk`Pending install`,`Pending uninstall`, dan`Installed`.

> **Note**
>
> Jika pengguna Anda mengamati bahwa bundel aplikasi yang baru diinstal melalui Aplikasi Terkelola tidak diaktifkan lisensi, Anda dapat melakukan WorkSpace reboot manual. Pengguna Anda dapat mulai menggunakan aplikasi tersebut setelah reboot. Untuk dukungan tambahan, hubungi AWSSupport.

Mengelola WorkSpaces dimodifikasi menggunakan Kelola aplikasi

Setelah menginstal atau menghapus bundel aplikasi pada Anda WorkSpaces, tindakan berikut dapat memengaruhi konfigurasi yang ada.

- Kembalikan a WorkSpace - Memulihkan WorkSpace membuat ulang volume root dan volume pengguna, berdasarkan snapshot terbaru dari volume ini yang dibuat saat sehat. WorkSpace WorkSpace Snapshot lengkap diambil setiap 12 jam. Untuk informasi selengkapnya, lihat

Memulihkan file WorkSpace. Pastikan Anda menunggu setidaknya 12 jam sebelum memulihkan WorkSpaces yang telah dimodifikasi menggunakan Kelola aplikasi. Memulihkan WorkSpaces sebelum snapshot lengkap berikutnya, yang dimodifikasi menggunakan Kelola aplikasi, akan menghasilkan hal berikut:

- Bundel aplikasi yang diinstal pada Anda WorkSpaces menggunakan alur kerja Kelola aplikasi akan dihapus dari Anda WorkSpaces tetapi lisensi akan tetap diaktifkan dan Anda WorkSpaces akan ditagih untuk aplikasi tersebut. Untuk mendapatkan kembali bundel aplikasi tersebut, WorkSpaces Anda perlu menjalankan alur kerja Kelola aplikasi lagi, hapus instalan aplikasi untuk memulai yang baru, dan kemudian instal lagi.
- Bundel aplikasi yang telah dihapus dari alur kerja Anda WorkSpaces menggunakan Kelola aplikasi akan kembali pada Anda. WorkSpaces Namun, bundel aplikasi tersebut tidak akan berfungsi dengan baik karena aktivasi lisensi akan hilang. Untuk menyingkirkan bundel aplikasi tersebut, jalankan uninstall bundel aplikasi tersebut secara manual dari bundel aplikasi Anda. WorkSpaces

- Membangun kembali WorkSpace - Membangun WorkSpace kembali sebuah menciptakan volume root. Untuk informasi selengkapnya, lihat Membangun kembali a. WorkSpace Membangun kembali aplikasi Anda WorkSpaces yang telah dimodifikasi menggunakan Kelola aplikasi akan menghasilkan hal berikut:
  - Bundel aplikasi yang diinstal pada Anda WorkSpaces menggunakan alur kerja Kelola aplikasi akan dihapus dan dinonaktifkan dari Anda. WorkSpaces Untuk mendapatkan kembali aplikasi tersebut, WorkSpaces Anda perlu menjalankan alur kerja Kelola aplikasi lagi.
  - Bundel aplikasi yang telah dihapus dari alur kerja Anda WorkSpaces melalui Kelola aplikasi akan diinstal dan diaktifkan pada Anda. WorkSpaces Untuk menghapus bundel aplikasi tersebut dari Anda WorkSpaces, Anda perlu menjalankan alur kerja Kelola aplikasi lagi.
- Migrasi a WorkSpace - Proses migrasi membuat ulang WorkSpace dengan menggunakan volume root baru dari gambar bundel target dan volume pengguna dari snapshot terakhir yang tersedia dari aslinya. WorkSpace Sebuah baru WorkSpace dengan WorkSpace ID baru dibuat. Untuk informasi selengkapnya, lihat Memigrasi WorkSpace Migrasi Anda WorkSpaces yang telah dimodifikasi menggunakan Kelola aplikasi akan menghasilkan hal berikut:
  - Semua bundel aplikasi dari sumber WorkSpaces akan dihapus dan dinonaktifkan. Tujuan baru WorkSpaces akan mewarisi aplikasi dari WorkSpaces bundel tujuan. Bundel WorkSpaces aplikasi sumber akan ditagih selama sebulan penuh tetapi bundel aplikasi pada bundel tujuan akan memiliki tagihan pro-rating.

Memodifikasi WorkSpace

Setelah meluncurkan WorkSpace, Anda dapat memodifikasi konfigurasinya dengan tiga cara:

- Anda dapat mengubah ukuran volume root nya (untuk Windows, drive C; untuk Linux,/) dan volume penggunanya (untuk Windows, drive D; untuk Linux /home).
- Anda dapat mengubah tipe komputasinya untuk memilih paket baru.
- Anda dapat memodifikasi protokol streaming menggunakan AWS CLI atau Amazon WorkSpaces API jika Anda WorkSpace dibuat dengan bundel PCoIP.

Untuk melihat status modifikasi saat ini WorkSpace, pilih panah untuk menampilkan detail lebih lanjut tentang itu WorkSpace. Nilai yang mungkin untuk Status adalah Mengubah komputasi, Mengubah Penyimpanan, dan Tidak ada.

Jika Anda ingin memodifikasi WorkSpace, itu harus memiliki status `AVAILABLE` atau`STOPPED`. Anda tidak dapat mengubah ukuran volume dan jenis komputasi secara bersamaan.

Mengubah ukuran volume atau jenis komputasi a WorkSpace akan mengubah tingkat penagihan untuk. WorkSpace

Untuk mengizinkan pengguna mengubah volume dan tipe komputasinya sendiri, lihat Aktifkan kemampuan WorkSpace manajemen swalayan untuk pengguna Anda.

Ubah ukuran volume

Anda dapat meningkatkan ukuran root dan volume pengguna untuk WorkSpace, hingga 2000 GB masing-masing. WorkSpace root dan volume pengguna datang dalam grup set yang tidak dapat diubah. Grup yang tersedia adalah:

[Root (GB), Pengguna (GB)]
[80, 10]
[80, 50]
[80, 100]
[175 hingga 2000, 100 hingga 2000]

Anda dapat memperluas root dan volume pengguna apakah mereka dienkripsi atau tidak dienkripsi, serta Anda dapat memperluas kedua volume sekali dalam periode 6 jam. Namun, Anda tidak dapat meningkatkan ukuran root dan volume pengguna secara bersamaan. Untuk informasi selengkapnya, lihat Keterbatasan untuk Meningkatkan Volume.

> **Note**
>
> Saat Anda memperluas volume untuk a WorkSpace, WorkSpaces secara otomatis memperluas partisi volume dalam Windows atau Linux. Ketika proses selesai, Anda harus me-reboot agar perubahan diterapkan. WorkSpace

Untuk memastikan bahwa data Anda dipertahankan, Anda tidak dapat mengurangi ukuran root atau volume pengguna setelah Anda meluncurkan file WorkSpace. Sebagai gantinya, pastikan Anda menentukan ukuran minimum untuk volume ini saat meluncurkan file WorkSpace. Anda dapat meluncurkan Nilai, Standar, Kinerja, Daya, atau PowerPro WorkSpace dengan minimal 80 GB untuk volume root dan 10 GB untuk volume pengguna. Anda dapat meluncurkan Graphics.g4dn, GraphicsPro .g4dn, Graphics, atau GraphicsPro WorkSpace dengan minimal 100 GB untuk volume root dan 100 GB untuk volume pengguna.

Sementara peningkatan ukuran WorkSpace disk sedang berlangsung, pengguna dapat melakukan sebagian besar tugas pada mereka WorkSpace. Namun, mereka tidak dapat mengubah jenis WorkSpace komputasi mereka, mengganti mode WorkSpace berjalan, membangun kembali mereka WorkSpace, atau reboot (restart) mereka. WorkSpace

> **Note**
>
> Jika Anda ingin pengguna Anda dapat menggunakannya WorkSpaces saat peningkatan ukuran disk sedang berlangsung, pastikan WorkSpaces memiliki status `AVAILABLE` alih-alih `STOPPED` sebelum Anda mengubah ukuran volume. WorkSpaces Jika ya`STOPPED`, WorkSpaces mereka tidak dapat dimulai saat peningkatan ukuran disk sedang berlangsung.

Dalam kebanyakan kasus, proses peningkatan ukuran disk mungkin memakan waktu hingga dua jam. Namun, jika Anda memodifikasi ukuran volume untuk sejumlah besar WorkSpaces, prosesnya bisa memakan waktu lebih lama. Jika Anda memiliki sejumlah besar WorkSpaces untuk dimodifikasi, kami sarankan AWS Support untuk menghubungi untuk bantuan.

Keterbatasan untuk meningkatkan volume

- Anda hanya dapat mengubah ukuran volume SSD.
- Ketika Anda meluncurkan WorkSpace, Anda harus menunggu 6 jam sebelum Anda dapat memodifikasi ukuran volumenya.
- Anda tidak dapat meningkatkan ukuran root dan volume pengguna pada saat yang sama. Untuk meningkatkan volume root, Anda harus terlebih dahulu mengubah volume pengguna menjadi 100 GB. Setelah diubah, kemudian Anda dapat memperbarui volume root untuk setiap nilai antara 175 dan 2000 GB. Setelah volume root diubah ke nilai apa pun antara 175 dan 2000 GB, kemudian Anda dapat memperbarui volume pengguna lebih lanjut, ke nilai apa pun antara 100 dan 2000 GB.

  > **Note**
  >
  > Jika Anda ingin meningkatkan kedua volume, Anda harus menunggu 20-30 menit agar operasi pertama selesai sebelum Anda dapat memulai operasi kedua.

- Kecuali jika WorkSpace adalah Graphics.g4dn, GraphicsPro .g4dn, Graphics, atau GraphicsPro WorkSpace, volume root tidak boleh kurang dari 175 GB ketika volume pengguna 100 GB. Graphics.g4dn, GraphicsPro .g4dn, Graphics, dan GraphicsPro WorkSpaces dapat memiliki volume root dan pengguna keduanya diatur ke minimum 100 GB.
- Jika volume pengguna adalah 50 GB, Anda tidak dapat memperbarui volume root untuk apa pun selain 80 GB. Jika volume root 80 GB, volume pengguna hanya dapat 10, 50, atau 100 GB.

Untuk memodifikasi volume root dari WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih WorkSpace dan pilih Tindakan, Ubah volume root. .
4. Di bawah ukuran volume Root, pilih ukuran volume atau pilih Kustom untuk memasukkan ukuran volume khusus.
5. Pilih Simpan perubahan.
6. Ketika peningkatan ukuran disk selesai, Anda harus me-reboot agar perubahan diterapkan. WorkSpace Untuk menghindari kehilangan data, pastikan pengguna menyimpan file yang terbuka sebelum Anda reboot file WorkSpace.

Untuk memodifikasi volume pengguna dari WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih WorkSpace dan pilih Tindakan, Ubah volume pengguna. .
4. Di bawah Ukuran volume pengguna, pilih ukuran volume atau pilih Kustom untuk memasukkan ukuran volume khusus.
5. Pilih Simpan perubahan.
6. Ketika peningkatan ukuran disk selesai, Anda harus me-reboot agar perubahan diterapkan. WorkSpace Untuk menghindari kehilangan data, pastikan pengguna menyimpan file yang terbuka sebelum Anda reboot file WorkSpace.

Untuk mengubah ukuran volume a WorkSpace

Gunakan modify-workspace-propertiesperintah dengan `UserVolumeSizeGib` properti `RootVolumeSizeGib` atau.

Ubah jenis komputasi

Anda dapat beralih WorkSpace antara tipe Standar, Daya, Kinerja, dan PowerPro komputasi. Untuk informasi selengkapnya tentang jenis komputasi ini, lihat Amazon WorkSpaces Bundles.

> **Note**
>
> - Anda dapat mengubah jenis komputasi dari Graphics.g4dn menjadi .g4dn, atau dari.g4dn ke Graphics.g4dn GraphicsPro. GraphicsPro Anda tidak dapat mengubah jenis komputasi Graphics.g4dn dan.g4dn ke nilai lainnya. GraphicsPro
> - Bundel grafis tidak lagi didukung setelah 30 November 2023. Kami merekomendasikan untuk memigrasikan paket Anda WorkSpaces ke Graphics.g4dn. Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.
> - Anda tidak dapat mengubah jenis komputasi Grafik dan GraphicsPro nilai lainnya.

Saat Anda meminta perubahan komputasi, WorkSpaces reboot WorkSpace menggunakan jenis komputasi baru. WorkSpaces mempertahankan sistem operasi, aplikasi, data, dan pengaturan penyimpanan untuk. WorkSpace

Anda dapat meminta jenis komputasi yang lebih besar sekali dalam periode 6 jam atau jenis komputasi yang lebih kecil setiap 30 hari sekali. Untuk yang baru diluncurkan WorkSpace, Anda harus menunggu 6 jam sebelum meminta jenis komputasi yang lebih besar.

Ketika perubahan jenis WorkSpace komputasi sedang berlangsung, pengguna terputus dari mereka WorkSpace, dan mereka tidak dapat menggunakan atau mengubah. WorkSpace Secara otomatis reboot selama proses perubahan jenis komputasi. WorkSpace

> **Important**
>
> Untuk menghindari kehilangan data, pastikan pengguna menyimpan dokumen terbuka dan file aplikasi lainnya sebelum Anda mengubah jenis WorkSpace komputasi.

Proses perubahan tipe komputasi mungkin memakan waktu hingga satu jam.

Untuk mengubah tipe komputasi WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih WorkSpace dan pilih Actions, Modify compute type.
4. Di bawah Jenis komputasi, pilih jenis komputasi.
5. Pilih Simpan perubahan.

Untuk mengubah tipe komputasi WorkSpace

Gunakan modify-workspace-propertiesperintah dengan `ComputeTypeName` properti.

Memodifikasi protokol

Jika Anda WorkSpace dibuat dengan bundel PCoIP, Anda dapat memodifikasi protokol streaming mereka menggunakan AWS CLI atau Amazon API. WorkSpaces Ini memungkinkan Anda untuk memigrasikan protokol menggunakan protokol yang sudah ada WorkSpace tanpa menggunakan fitur WorkSpace migrasi. Ini juga memungkinkan Anda untuk menggunakan Protokol WorkSpaces Streaming (WSP) dan mempertahankan volume root Anda tanpa membuat ulang PCoIP yang ada WorkSpaces selama proses migrasi.

- Anda hanya dapat memodifikasi protokol Anda jika Anda WorkSpace dibuat dengan bundel PCoIP.

- Sebelum Anda memodifikasi protokol ke WSP, pastikan bahwa Anda WorkSpace memenuhi persyaratan berikut untuk WorkSpace WSP.
  - WorkSpaces Klien Anda mendukung WSP
  - Wilayah tempat Anda WorkSpace digunakan mendukung WSP
  - Alamat IP dan persyaratan port untuk WSP terbuka. Untuk informasi selengkapnya, lihat alamat IP dan persyaratan port untuk WorkSpaces.
  - Pastikan bundel Anda saat ini tersedia dengan WSP.
  - Untuk pengalaman terbaik dengan konferensi video, kami sarankan menggunakan Power atau PowerPro bundel saja.

> **Note**
>
> - Kami sangat menyarankan pengujian dengan non-produksi Anda WorkSpaces sebelum Anda mulai mengubah protokol.
> - Jika Anda memodifikasi protokol dari PCoIP ke WSP, dan kemudian memodifikasi protokol kembali ke PCoIP, Anda tidak akan dapat terhubung melalui Akses Web. WorkSpaces

Untuk mengubah protokol dari WorkSpace

1. [Opsional] Reboot Anda WorkSpace dan tunggu sampai dalam `AVAILABLE` status sebelum memodifikasi protokol.
2. [Opsional] Gunakan `describe-workspaces` perintah untuk membuat daftar WorkSpace properti. Pastikan bahwa itu dalam `AVAILABLE` keadaan dan saat `Protocol` ini akurat.
3. Gunakan `modify-workspace-properties` perintah dan modifikasi `Protocols` properti dari `PCOIP` ke`WSP`, atau sebaliknya.

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> `Protocols`Properti ini peka huruf besar/kecil. Pastikan Anda menggunakan `PCOIP` atau `WSP`

4. Setelah Anda menjalankan perintah, dibutuhkan waktu hingga 20 menit WorkSpace untuk reboot dan menyelesaikan konfigurasi yang diperlukan.
5. Gunakan `describe-workspaces` perintah lagi untuk membuat daftar WorkSpace properti dan memverifikasi bahwa itu dalam `AVAILABLE` keadaan dan `Protocols` properti saat ini telah diubah ke protokol yang benar.

> **Note**
>
> - WorkSpaceMemodifikasi protokol tidak akan memperbarui deskripsi bundel di konsol. Deskripsi Launch Bundle tidak akan berubah.
> - Jika WorkSpace tetap dalam `UNHEALTHY` keadaan setelah 20 menit, reboot WorkSpace di konsol.

6. Anda sekarang dapat terhubung ke Anda WorkSpace.

Sesuaikan WorkSpace branding

Amazon WorkSpaces memungkinkan Anda untuk membuat WorkSpaces pengalaman yang akrab bagi pengguna Anda dengan menggunakan API untuk menyesuaikan tampilan halaman login Anda WorkSpace dengan logo merek Anda sendiri, informasi dukungan TI, tautan lupa kata sandi, dan pesan masuk. Branding Anda akan ditampilkan kepada pengguna Anda di halaman WorkSpace login mereka, bukan WorkSpaces branding default.

Klien berikut didukung:

- Windows
- Linux
- Android
- macOS
- iOS

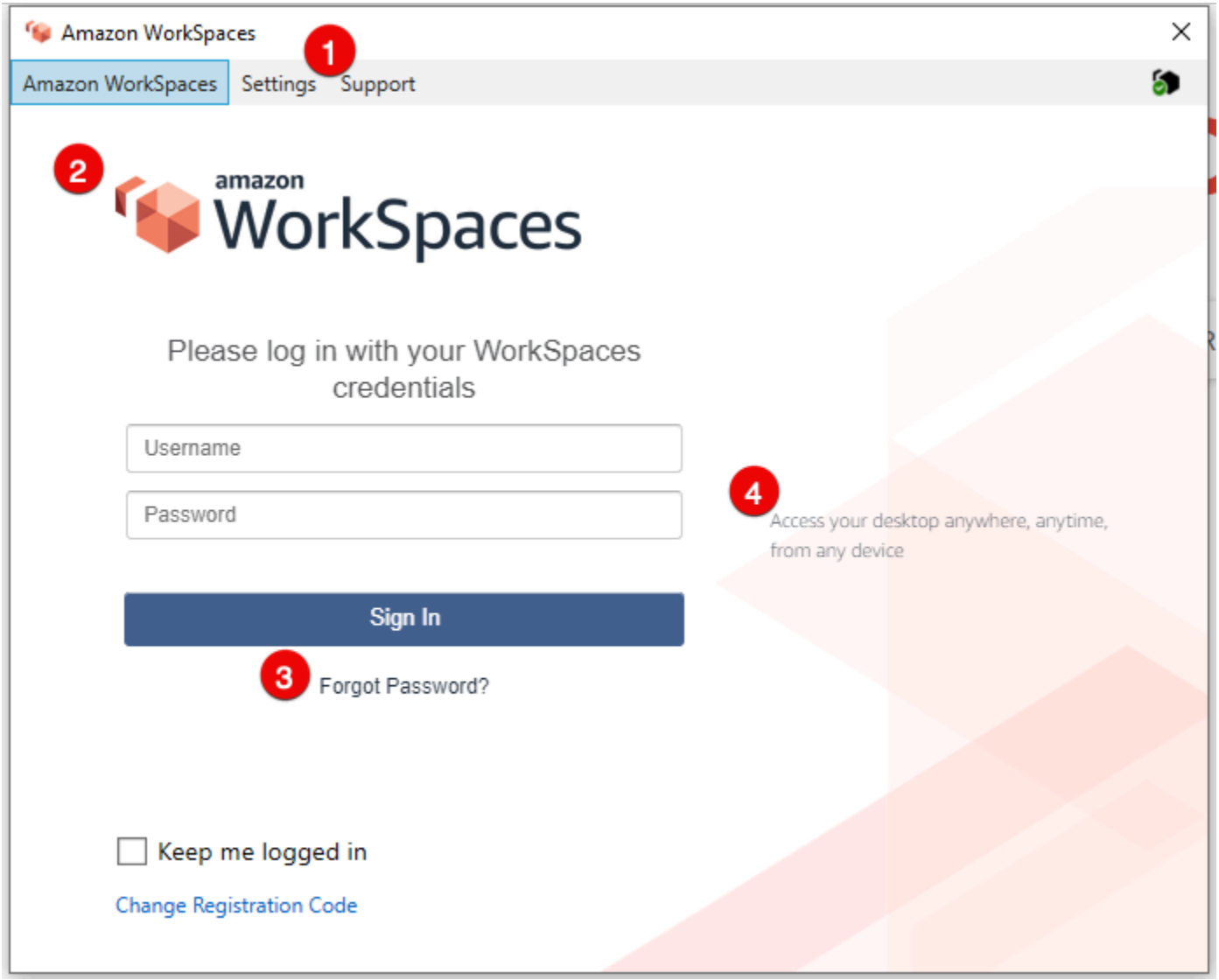
- Akses Web

> **Note**
>
> Untuk memodifikasi elemen branding menggunakan ClientBranding API diAWS GovCloud (US) Region, gunakan versi WorkSpaces klien yaitu 5.10.0.

Impor merek khusus

Untuk mengimpor kustomisasi branding klien Anda, gunakan tindakan`ImportClientBranding`, yang mencakup elemen-elemen berikut. Lihat referensi ImportClientBranding API untuk informasi selengkapnya.

> **Important**
>
> Atribut branding klien dihadapi publik. Pastikan Anda tidak menyertakan informasi sensitif.



1. Tautan Dukungan
2. Logo
3. Lupa tautan kata sandi
4. Pesan login

Elemen branding kustom

Elemen branding	Deskripsi	Persyaratan dan rekomendasi
Tautan Dukungan	Memungkinkan Anda untuk menentukan link email dukungan bagi pengguna	• Untuk setiap jenis platform, `SupportLink` parameter `SupportEmail` dan

Elemen branding	Deskripsi	Persyaratan dan rekomendasi
	untuk menghubungi untuk bantuan dengan mereka WorkSpaces. Anda dapat menggunakan `SupportEmail` atribut atau memberikan link ke halaman dukungan Anda menggunakan `SupportLink` atribut.	saling eksklusif. Anda dapat menentukan satu parameter untuk setiap jenis platform, tetapi tidak keduanya. • Email default adalah`workspaces-feedback@amazon.com` . • Panjang batasan: Panjang minimum 1. Panjang maksimum 200.

Logo	Memungkinkan Anda menyesuaikan logo organisasi Anda menggunakan `Logo` atribut.	• Satu-satunya format gambar yang diterima adalah objek data biner yang dikonversi dari `.png` file.
		• Resolusi yang direkomendasikan:
		  • Android: 978 x 190
		  • Desktop: 319 x 55
		  • iOS @2x: 110 x 200
		  • iOS @3x: 1650 x 300

Lupa tautan kata sandi	Memungkinkan Anda menambahkan alamat web menggunakan ForgotPasswordLink atribut yang dapat dikunjungi pengguna jika mereka lupa kata sandi mereka WorkSpace.	Batasan Panjang: Panjang minimum 1. Panjang maksimum 200.

Elemen branding	Deskripsi	Persyaratan dan rekomendasi
Pesan login	Memungkinkan Anda menyesuaikan pesan menggunakan `LoginMessage` atribut pada layar masuk.	• Batasan Panjang: Panjang minimum sebesar 0. Panjang maksimum 2000 karakter untuk integrasi dengan tag HTML dan ukuran font yang berbeda. Untuk kasus default tanpa tag HTML, disarankan untuk menyimpan pesan login di bawah 600 karakter. • Tag HTML didukung: `a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

Berikut ini adalah contoh cuplikan kode untuk digunakan. ImportClientBranding

AWSCLI Versi 2

> **Warning**
>
> Mengimpor merek khusus menimpa atribut, di dalam platform itu, yang Anda tentukan dengan data kustom Anda. Ini juga menimpa atribut yang tidak Anda tentukan dengan nilai atribut pencitraan merek kustom default. Anda harus menyertakan data untuk atribut apa pun yang tidak ingin Anda timpa.

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

File impor JSON akan terlihat seperti kode contoh berikut:

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

Contoh cuplikan kode Java berikut mengubah gambar logo menjadi string yang dikodekan base64:

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

Contoh cuplikan kode Python berikut mengubah gambar logo menjadi string yang dikodekan base64:

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> Mengimpor merek khusus menimpa atribut, di dalam platform itu, yang Anda tentukan dengan data kustom Anda. Ini juga menimpa atribut yang tidak Anda tentukan dengan nilai atribut pencitraan merek kustom default. Anda harus menyertakan data untuk atribut apa pun yang tidak ingin Anda timpa.

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> Mengimpor merek khusus menimpa atribut, di dalam platform itu, yang Anda tentukan dengan data kustom Anda. Ini juga menimpa atribut yang tidak Anda tentukan dengan nilai atribut pencitraan merek kustom default. Anda harus menyertakan data untuk atribut apa pun yang tidak ingin Anda timpa.

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
```

```
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

Untuk melihat pratinjau halaman login, luncurkan WorkSpaces aplikasi atau halaman login web.

> **Note**
>
> Perubahan mungkin memakan waktu hingga 1 menit untuk muncul.

Jelaskan merek khusus

Untuk melihat detail kustomisasi branding klien yang Anda miliki saat ini, gunakan tindakan`DescribeCustomBranding`. Berikut ini adalah contoh script untuk menggunakan DescribeClientBranding. Lihat referensi DescribeClientBranding API untuk informasi selengkapnya.

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

Hapus merek khusus

Untuk menghapus kustomisasi merek klien Anda, gunakan tindakan`DeleteCustomBranding`. Berikut ini adalah contoh script untuk menggunakan DeleteClientBranding. Lihat referensi DeleteClientBranding API untuk informasi selengkapnya.

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> Perubahan mungkin memakan waktu hingga 1 menit untuk muncul.

WorkSpaces Sumber daya tag

Anda dapat mengatur dan mengelola sumber daya untuk Anda WorkSpaces dengan menetapkan metadata Anda sendiri ke setiap sumber daya dalam bentuk tag. Anda menentukan kunci dan nilai untuk setiap tanda. Kunci dapat berupa kategori umum, seperti "proyek," "pemilik," atau "lingkungan," dengan nilai terkait tertentu. Menggunakan tanda adalah cara sederhana tetapi andal 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 tag yang sudah ada WorkSpace pada 15 Juli, tag tidak akan muncul di laporan alokasi biaya hingga 1 Agustus. Untuk informasi selengkapnya, lihat Menggunakan Tag Alokasi Biaya dalam Panduan Pengguna AWS Billing.

> **Note**
>
> Untuk melihat tag WorkSpaces sumber daya Anda di Cost Explorer, Anda harus mengaktifkan tag yang telah diterapkan ke WorkSpaces sumber daya Anda dengan mengikuti petunjuk dalam Mengaktifkan Tag Alokasi Biaya yang Ditentukan Pengguna di Panduan Pengguna. AWS Billing
>
> Meskipun tanda muncul 24 jam setelah aktivasi, diperlukan waktu 4 hingga 5 hari agar nilai yang terkait dengan tanda tersebut muncul di Cost Explorer. Selain itu, untuk menampilkan dan menyediakan data biaya di Cost Explorer, WorkSpaces sumber daya yang telah ditandai harus dikenakan biaya selama waktu itu. Cost Explorer hanya menampilkan data biaya dari saat tanda diaktifkan dan seterusnya. Tidak ada data riwayat yang tersedia saat ini.

Sumber daya yang dapat Anda tandai

- Anda dapat menambahkan tag ke sumber daya berikut saat Anda membuatnya—WorkSpaces, gambar yang diimpor, dan grup kontrol akses IP.
- Anda dapat menambahkan tag ke sumber daya yang ada dari jenis berikut—WorkSpaces, direktori terdaftar, bundel kustom, gambar, dan grup kontrol akses IP.

Pembatasan tanda

- Jumlah maksimum tanda per sumber daya—50
- Panjang kunci maksimum – 127 karakter Unicode
- Panjang nilai maksimum – 255 karakter Unicode
- Kunci dan nilai tanda 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 menggunakan prefiks `aws:` atau `aws:workspaces:` pada nama atau nilai tanda Anda, karena hal ini khusus untuk penggunaan AWS. Anda tidak dapat mengedit atau menghapus nama atau nilai tanda dengan prefiks ini.

Untuk memperbarui tag untuk sumber daya yang ada menggunakan konsol (direktori WorkSpaces, atau grup kontrol akses IP)

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih salah satu jenis sumber daya berikut: Direktori WorkSpaces, atau Kontrol Akses IP.
3. Pilih sumber daya untuk membuka halaman detailnya.
4. Lakukan salah satu atau beberapa hal berikut:
   - Untuk memperbarui tanda, edit nilai Kunci dan Nilai.
   - Untuk menambahkan tanda baru, pilih Tambahkan tanda lalu edit nilai Kunci dan Nilai.
   - Untuk menghapus tanda, pilih ikon hapus (X) disebelah tanda.
5. Setelah Anda selesai memperbarui tanda, pilih Simpan.

Untuk memperbarui tanda untuk sumber daya yang ada menggunakan konsol tersebut (citra atau paket)

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih salah satu tipe sumber daya berikut: Paket atau Citra.
3. Pilih sumber daya untuk membuka halaman detailnya.
4. Di bagian Tanda, pilih Kelola tanda.
5. Lakukan salah satu atau beberapa hal berikut:

- Untuk memperbarui tanda, edit nilai Kunci dan Nilai.
- Untuk menambahkan tanda, pilih Tambahkan tanda baru lalu edit nilai Kunci dan Nilai.
- Untuk menghapus tanda, pilih Hapus di samping tanda.

6. Setelah selesai memperbarui tanda, pilih Simpan perubahan.

Untuk memperbarui tanda untuk sumber daya yang ada gunakan AWS CLI

Gunakan perintah buat-tanda dan hapus-tanda.

WorkSpace pemeliharaan

Kami menyarankan Anda untuk mempertahankannya WorkSpaces secara teratur. WorkSpaces menjadwalkan jendela pemeliharaan default untuk Anda WorkSpaces. Selama jendela pemeliharaan, WorkSpace menginstal pembaruan penting dari Amazon WorkSpaces dan reboot seperlunya. Jika tersedia, pembaruan sistem operasi juga diinstal dari server pembaruan OS yang WorkSpace dikonfigurasi untuk digunakan. Selama pemeliharaan, Anda WorkSpaces mungkin tidak tersedia.

Secara default, Windows Anda WorkSpaces dikonfigurasi untuk menerima pembaruan dari Pembaruan Windows. Untuk mengonfigurasi mekanisme pembaruan otomatis Anda sendiri untuk Windows, lihat dokumentasi untuk Layanan Pembaruan Server Windows (WSUS) dan Manajer konfigurasi.

Persyaratan

Anda WorkSpaces harus memiliki akses ke internet sehingga Anda dapat menginstal pembaruan ke sistem operasi dan menyebarkan aplikasi. Untuk informasi selengkapnya, lihat the section called “Akses internet”.

Jendela pemeliharaan untuk AlwaysOn WorkSpaces

Untuk AlwaysOn WorkSpaces, jendela pemeliharaan ditentukan oleh pengaturan sistem operasi. Standarnya adalah periode empat jam dari 00h00 hingga 04h00, di zona waktu, setiap Minggu pagi. WorkSpace Secara default, zona waktu dari sebuah AlwaysOn WorkSpace adalah zona waktu AWS Wilayah untuk WorkSpace. Namun, jika Anda terhubung dari Wilayah lain dan pengalihan zona waktu diaktifkan, dan kemudian Anda memutuskan sambungan, zona waktu WorkSpace diperbarui ke zona waktu Wilayah tempat Anda terhubung.

Anda dapat menonaktifkan pengalihan zona waktu untuk Windows WorkSpaces menggunakan Kebijakan Grup. Anda dapat menonaktifkan pengalihan zona waktu untuk Linux WorkSpaces dengan menggunakan conf Agen PCoIP.

Untuk Windows WorkSpaces, Anda dapat mengonfigurasi jendela pemeliharaan menggunakan Kebijakan Grup; lihat Mengkonfigurasi Pengaturan Kebijakan Grup untuk Pembaruan Otomatis. Anda tidak dapat mengkonfigurasi jendela pemeliharaan untuk Linux WorkSpaces.

Jendela pemeliharaan untuk AutoStop WorkSpaces

AutoStop WorkSpaces dimulai secara otomatis sebulan sekali untuk menginstal pembaruan penting. Dimulai pada hari Senin ketiga setiap bulan, dan hingga dua minggu, jendela pemeliharaan terbuka setiap hari dari sekitar 00h00 hingga 05h00, di zona waktu Wilayah untuk. AWS WorkSpace WorkSpace Dapat dipertahankan pada satu hari di jendela pemeliharaan. Selama jendela ini, hanya WorkSpaces lebih dari 7 hari yang dipertahankan.

Selama periode waktu ketika WorkSpace sedang menjalani pemeliharaan, keadaan WorkSpace diatur ke`MAINTENANCE`.

Meskipun Anda tidak dapat mengubah zona waktu yang digunakan untuk pemeliharaan AutoStop WorkSpaces, Anda dapat menonaktifkan jendela pemeliharaan untuk Anda AutoStop WorkSpaces sebagai berikut. Jika Anda menonaktifkan mode pemeliharaan, WorkSpaces Anda tidak di-reboot dan tidak memasuki status. `MAINTENANCE`

Cara menonaktifkan mode pemeliharaan

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori Anda, dan pilih Tindakan, Perbarui Detail.
4. Perluas Mode Pemeliharaan.
5. Untuk mengaktifkan pembaruan otomatis, pilih Diaktifkan. Jika Anda lebih suka mengelola pembaruan secara manual, pilih Dinonaktifkan.
6. Pilih Perbarui dan Keluar.

Pemeliharaan manual

Jika Anda mau, Anda dapat mempertahankan WorkSpaces jadwal Anda sendiri. Saat Anda melakukan tugas pemeliharaan, kami sarankan Anda mengubah status WorkSpace menjadi Pemeliharaan. Setelah selesai, ubah status WorkSpace menjadi Tersedia.

Ketika a WorkSpace dalam keadaan Pemeliharaan, perilaku berikut terjadi:

- The WorkSpace tidak menanggapi permintaan untuk reboot, menghentikan, memulai, atau membangun kembali.
- Pengguna tidak dapat masuk ke file WorkSpace.
- An AutoStop WorkSpace tidak hibernasi.

Untuk mengubah status WorkSpace menggunakan konsol

> **Note**
>
> Untuk mengubah status a WorkSpace, WorkSpace harus dalam keadaan Tersedia. Pengaturan Ubah status tidak tersedia saat a WorkSpace tidak dalam status Tersedia.

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih Anda WorkSpace, dan pilih Tindakan, Ubah status.
4. Di bawah Ubah status, pilih Tersedia atau Pemeliharaan.
5. Pilih Save (Simpan).

Untuk mengubah keadaan WorkSpace menggunakan AWS CLI

Gunakan perintah modify-workspace-state.

Terenkripsi WorkSpaces

WorkSpaces terintegrasi dengan AWS Key Management Service (AWS KMS). Ini memungkinkan Anda untuk mengenkripsi volume penyimpanan WorkSpaces menggunakan AWS KMS Key.

Ketika Anda meluncurkan WorkSpace, Anda dapat mengenkripsi volume root (untuk Microsoft Windows, drive C; untuk Linux,/) dan volume pengguna (untuk Windows, drive D; untuk Linux, /home). Melakukannya memastikan bahwa data yang disimpan saat istirahat, disk I/O ke volume, dan snapshot yang dibuat dari volume semuanya dienkripsi.

> **Note**
>
> Selain mengenkripsi Anda WorkSpaces, Anda juga dapat menggunakan enkripsi endpoint FIPS di Wilayah AS tertentu. AWS Untuk informasi selengkapnya, lihat Siapkan Amazon WorkSpaces untuk otorisasi FedRAMP atau kepatuhan DoD SRG.

Daftar Isi

Prasyarat

Anda memerlukan AWS KMS kunci sebelum Anda dapat memulai proses enkripsi. Kunci KMS ini dapat berupa Kunci KMS AWSterkelola untuk Amazon WorkSpaces (aws/ruang kerja) atau Kunci KMS yang dikelola pelanggan simetris.

- AWSKunci KMS terkelola - Pertama kali Anda meluncurkan yang tidak terenkripsi WorkSpace dari WorkSpaces konsol di Wilayah, Amazon WorkSpaces secara otomatis membuat Kunci KMS AWS terkelola (aws/ruang kerja) di akun Anda. Anda dapat memilih Kunci KMS AWS terkelola ini untuk mengenkripsi volume pengguna dan root Anda. WorkSpace Untuk detailnya, lihat Ikhtisar WorkSpaces enkripsi menggunakan AWS KMS.

  Anda dapat melihat Kunci KMS AWS terkelola ini, termasuk kebijakan dan hibah, dan dapat melacak penggunaannya di AWS CloudTrail log, tetapi Anda tidak dapat menggunakan atau

mengelola Kunci KMS ini. Amazon WorkSpaces membuat dan mengelola Kunci KMS ini. Hanya Amazon yang WorkSpaces dapat menggunakan Kunci KMS ini, dan WorkSpaces dapat menggunakannya hanya untuk mengenkripsi WorkSpaces sumber daya di akun Anda.

AWSKMS Key yang dikelola, termasuk yang WorkSpaces didukung Amazon, diputar setiap tiga tahun. Untuk detailnya, lihat Rotating AWS KMS Key di Panduan AWS Key Management Service Pengembang.

- Kunci KMS yang dikelola pelanggan - Atau, Anda dapat memilih KMS Key yang dikelola pelanggan simetris yang Anda buat menggunakan. AWS KMS Anda dapat melihat, menggunakan, dan mengelola Kunci KMS ini, termasuk menyetel kebijakannya. Untuk informasi selengkapnya tentang membuat Kunci KMS, lihat Membuat Kunci di Panduan AWS Key Management Service Pengembang. Untuk informasi selengkapnya tentang membuat Kunci KMS menggunakan AWS KMS API, lihat Bekerja dengan Kunci di Panduan AWS Key Management Service Pengembang.

  Kunci KMS yang dikelola pelanggan tidak diputar secara otomatis kecuali Anda memutuskan untuk mengaktifkan rotasi kunci otomatis. Untuk detailnya, lihat Rotating AWS KMS Keys di Panduan AWS Key Management Service Pengembang.

> **Important**
>
> Ketika Anda memutar KMS Keys secara manual, Anda harus menjaga KMS Key asli dan KMS Key baru diaktifkan sehingga AWS KMS dapat mendekripsi bahwa KMS Key asli WorkSpaces dienkripsi. Jika Anda tidak ingin mengaktifkan Kunci KMS asli, Anda harus membuat ulang WorkSpaces dan mengenkripsi mereka menggunakan Kunci KMS baru.

Anda harus memenuhi persyaratan berikut untuk menggunakan AWS KMS Kunci untuk mengenkripsi: WorkSpaces

- Kunci KMS harus simetris. Amazon WorkSpaces tidak mendukung KMS Keys asimetris. Untuk informasi tentang membedakan antara Kunci KMS simetris dan asimetris, lihat Mengidentifikasi Kunci KMS Simetris dan Asimetris di Panduan Pengembang. AWS Key Management Service
- Kunci KMS harus diaktifkan. Untuk menentukan apakah Kunci KMS diaktifkan, lihat Menampilkan Rincian Kunci KMS di Panduan PengembangAWS Key Management Service.
- Anda harus memiliki izin dan kebijakan yang benar terkait dengan Kunci KMS. Untuk informasi selengkapnya, lihat Bagian 2: Berikan izin tambahan WorkSpaces kepada administrator menggunakan kebijakan IAM.

Batas

- Anda tidak dapat mengenkripsi yang sudah ada WorkSpace. Anda harus mengenkripsi WorkSpace ketika Anda meluncurkannya.
- Membuat gambar kustom dari terenkripsi tidak WorkSpace didukung.
- Menonaktifkan enkripsi untuk terenkripsi saat WorkSpace ini tidak didukung.
- WorkSpaces diluncurkan dengan enkripsi volume root diaktifkan mungkin memakan waktu hingga satu jam untuk penyediaan.
- Untuk me-reboot atau membangun kembali terenkripsi WorkSpace, pertama-tama pastikan bahwa AWS KMS Kunci diaktifkan; jika tidak, menjadi tidak dapat digunakan. WorkSpace Untuk menentukan apakah Kunci KMS diaktifkan, lihat Menampilkan Rincian Kunci KMS di Panduan PengembangAWS Key Management Service.

Ikhtisar WorkSpaces enkripsi menggunakan AWS KMS

Saat Anda membuat WorkSpaces dengan volume terenkripsi, WorkSpaces gunakan Amazon Elastic Block Store (Amazon EBS) untuk membuat dan mengelola volume tersebut. Amazon EBS mengenkripsi volume Anda dengan kunci data menggunakan algoritme AES-256 standar industri. Baik Amazon EBS dan Amazon WorkSpaces menggunakan Kunci KMS Anda untuk bekerja dengan volume terenkripsi. Untuk informasi selengkapnya tentang enkripsi volume EBS, lihat Enkripsi Amazon EBS dalam Panduan Pengguna Amazon EC2 untuk Instans Windows.

Saat Anda meluncurkan WorkSpaces dengan volume terenkripsi, end-to-end prosesnya bekerja seperti ini:

1. Anda menentukan Kunci KMS yang akan digunakan untuk enkripsi serta pengguna dan direktori untuk. WorkSpace Tindakan ini membuat hibah yang memungkinkan WorkSpaces untuk menggunakan Kunci KMS Anda hanya untuk ini WorkSpace —yaitu, hanya untuk yang WorkSpace terkait dengan pengguna dan direktori yang ditentukan.
2. WorkSpaces membuat volume EBS terenkripsi untuk WorkSpace dan menentukan Kunci KMS untuk digunakan serta pengguna dan direktori volume. Tindakan ini membuat hibah yang memungkinkan Amazon EBS menggunakan Kunci KMS Anda hanya untuk ini WorkSpace dan volume—yaitu, hanya untuk yang WorkSpace terkait dengan pengguna dan direktori yang ditentukan, dan hanya untuk volume yang ditentukan.

3. Amazon EBS meminta kunci data volume yang dienkripsi di bawah Kunci KMS Anda dan menentukan pengenal keamanan Direktori Aktif (SID) WorkSpace pengguna dan ID AWS Directory Service direktori serta ID volume Amazon EBS sebagai konteks enkripsi.
4. AWS KMSmembuat kunci data baru, mengenkripsinya di bawah Kunci KMS Anda, dan kemudian mengirimkan kunci data terenkripsi ke Amazon EBS.
5. WorkSpaces menggunakan Amazon EBS untuk melampirkan volume terenkripsi ke Anda. WorkSpace Amazon EBS mengirimkan kunci data terenkripsi AWS KMS dengan `Decrypt`permintaan dan menentukan SID WorkSpace pengguna, ID direktori, dan ID volume, yang digunakan sebagai konteks enkripsi.
6. AWS KMSmenggunakan Kunci KMS Anda untuk mendekripsi kunci data, dan kemudian mengirimkan kunci data teks biasa ke Amazon EBS.
7. Amazon EBS menggunakan kunci data teks biasa untuk mengenkripsi semua data yang masuk ke dan dari volume terenkripsi. Amazon EBS menyimpan kunci data teks biasa di memori selama volume dilampirkan ke file. WorkSpace
8. Amazon EBS menyimpan kunci data terenkripsi (diterima diStep 4) dengan metadata volume untuk penggunaan di masa mendatang jika Anda me-reboot atau membangun kembali. WorkSpace
9. Saat Anda menggunakan file AWS Management Console untuk menghapus WorkSpace (atau menggunakan `TerminateWorkspaces`tindakan di WorkSpaces API), WorkSpaces dan Amazon EBS menghentikan hibah yang memungkinkan mereka menggunakan Kunci KMS Anda untuk itu. WorkSpace

WorkSpaces konteks enkripsi

WorkSpaces tidak menggunakan Kunci KMS Anda secara langsung untuk operasi kriptografi (seperti `Encrypt`,, `DecryptGenerateDataKey`, dll.), Yang WorkSpaces berarti tidak mengirim permintaan ke AWS KMS yang menyertakan konteks enkripsi. Namun, ketika Amazon EBS meminta kunci data terenkripsi untuk volume terenkripsi WorkSpaces (Step 3dalamIkhtisar WorkSpaces enkripsi menggunakan AWS KMS) Anda dan ketika meminta salinan teks biasa dari kunci data tersebut (Step 5), itu menyertakan konteks enkripsi dalam permintaan.

Konteks enkripsi menyediakan data terautentikasi tambahan(AAD) yang AWS KMS gunakan untuk memastikan integritas data. Konteks enkripsi juga ditulis ke file AWS CloudTrail log Anda, yang dapat membantu Anda memahami mengapa Kunci KMS yang diberikan digunakan. Amazon EBS menggunakan hal berikut ini untuk konteks enkripsi:

- Pengidentifikasi keamanan (SID) dari pengguna Active Directory yang terkait dengan WorkSpace
- ID direktori AWS Directory Service direktori yang terkait dengan WorkSpace
- ID volume Amazon EBS dari volume terenkripsi

Contoh berikut menunjukkan representasi JSON dari konteks enkripsi yang digunakan Amazon EBS:

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

Berikan WorkSpaces izin untuk menggunakan Kunci KMS atas nama Anda

Anda dapat melindungi WorkSpace data Anda di bawah Kunci KMS AWS terkelola untuk WorkSpaces (aws/ruang kerja) atau Kunci KMS yang dikelola pelanggan. Jika Anda menggunakan Kunci KMS yang dikelola pelanggan, Anda harus memberikan WorkSpaces izin untuk menggunakan Kunci KMS atas nama WorkSpaces administrator di akun Anda. Kunci KMS AWS terkelola untuk WorkSpaces memiliki izin yang diperlukan secara default.

Untuk mempersiapkan KMS Key yang dikelola pelanggan Anda untuk digunakan WorkSpaces, gunakan prosedur berikut.

1. Tambahkan WorkSpaces administrator Anda ke daftar pengguna kunci dalam kebijakan kunci KMS Key
2. Berikan izin tambahan WorkSpaces kepada administrator Anda dengan kebijakan IAM

WorkSpaces Administrator Anda juga memerlukan izin untuk menggunakannya WorkSpaces. Untuk informasi selengkapnya tentang izin ini, buka Identitas dan manajemen akses untuk WorkSpaces.

Bagian 1: Tambahkan WorkSpaces administrator sebagai pengguna utama

Untuk memberi WorkSpaces administrator izin yang mereka butuhkan, Anda dapat menggunakan AWS Management Console atau API. AWS KMS

Untuk menambahkan WorkSpaces administrator sebagai pengguna kunci untuk Kunci KMS (konsol)

1. Masuk ke AWS Management Console dan buka konsol AWS Key Management Service (AWS KMS) di https://console.aws.amazon.com/kms.

2. Untuk mengubahWilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Di panel navigasi, pilih Kunci yang dikelola pelanggan.
4. Pilih ID kunci atau alias KMS Key yang dikelola pelanggan pilihan Anda.
5. Pilih tab Kebijakan kunci. Di bawah Pengguna kunci, pilih Tambahkan.
6. Dalam daftar pengguna dan peran IAM, pilih pengguna dan peran yang sesuai dengan WorkSpaces administrator Anda, lalu pilih Tambah.

Untuk menambahkan WorkSpaces administrator sebagai pengguna kunci untuk Kunci KMS (API)

1. Gunakan GetKeyPolicyoperasi untuk mendapatkan kebijakan kunci yang ada, lalu simpan dokumen kebijakan ke file.
2. Buka dokumen kebijakan di editor teks pilihan Anda. Tambahkan pengguna IAM dan peran yang sesuai dengan WorkSpaces administrator Anda ke pernyataan kebijakan yang memberikan izin kepada pengguna utama. Kemudian simpan file.
3. Gunakan PutKeyPolicyoperasi untuk menerapkan kebijakan kunci ke Kunci KMS.

Bagian 2: Berikan izin tambahan WorkSpaces kepada administrator menggunakan kebijakan IAM

Jika Anda memilih Kunci KMS yang dikelola pelanggan untuk digunakan untuk enkripsi, Anda harus menetapkan kebijakan IAM yang WorkSpaces memungkinkan Amazon menggunakan Kunci KMS atas nama pengguna IAM di akun Anda yang meluncurkan terenkripsi. WorkSpaces Pengguna itu juga memerlukan izin untuk menggunakan Amazon WorkSpaces. Untuk informasi selengkapnya tentang membuat dan mengedit kebijakan pengguna IAM, lihat Mengelola Kebijakan IAM dalam Panduan Pengguna IAM dan Identitas dan manajemen akses untuk WorkSpaces.

WorkSpaces enkripsi membutuhkan akses terbatas ke Kunci KMS. Berikut ini adalah contoh kebijakan kunci yang dapat Anda gunakan. Kebijakan ini memisahkan prinsipal yang dapat mengelola AWS KMS Kunci dari mereka yang dapat menggunakannya. Sebelum Anda menggunakan kebijakan kunci contoh ini, ganti contoh akun ID dan nama pengguna IAM dengan nilai aktual dari akun Anda.

Pernyataan pertama cocok dengan default kebijakan kunci AWS KMS. Ini memberikan izin akun Anda untuk menggunakan kebijakan IAM untuk mengontrol akses ke Kunci KMS. Pernyataan kedua dan ketiga menentukan principal AWS dapat mengelola dan menggunakan kunci, masing-

masing. Pernyataan keempat mengaktifkan layanan AWS yang terintegrasi dengan AWS KMS untuk menggunakan kunci atas nama principal yang ditentukan. Pernyataan ini mengaktifkan layanan AWS untuk membuat dan mengelola pemberian. Pernyataan menggunakan elemen kondisi yang membatasi hibah pada Kunci KMS untuk yang dibuat oleh AWS layanan atas nama pengguna di akun Anda.

> **Note**
>
> Jika WorkSpaces administrator Anda menggunakan AWS Management Console untuk membuat WorkSpaces dengan volume terenkripsi, administrator memerlukan izin untuk membuat daftar alias dan kunci daftar (dan izin). `"kms:ListAliases"` `"kms:ListKeys"` Jika WorkSpaces administrator hanya menggunakan Amazon WorkSpaces API (bukan konsol), Anda dapat menghilangkan izin `"kms:ListAliases"` dan `"kms:ListKeys"` izin.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
```

```
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

Kebijakan IAM untuk pengguna atau peran yang mengenkripsi WorkSpace harus menyertakan izin penggunaan pada Kunci KMS yang dikelola pelanggan, serta akses ke. WorkSpaces Untuk memberikan WorkSpaces izin pengguna atau peran IAM, Anda dapat melampirkan kebijakan contoh berikut ke pengguna atau peran IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
```

```
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

Kebijakan IAM berikut ini diperlukan oleh pengguna untuk menggunakan AWS KMS. Ini memberi pengguna akses hanya-baca ke Kunci KMS bersama dengan kemampuan untuk membuat hibah.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Jika Anda ingin menentukan Kunci KMS dalam kebijakan Anda, gunakan kebijakan IAM yang serupa dengan yang berikut ini. Ganti contoh KMS Key ARN dengan yang valid.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Enkripsi WorkSpace

Untuk mengenkripsi WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Pilih Luncurkan WorkSpaces dan selesaikan tiga langkah pertama.
3. Untuk langkah WorkSpaces Konfigurasi, lakukan hal berikut:
   a. Pilih volume untuk mengenkripsi: Volume Root, Volume Pengguna, atau kedua volume.
   b. Untuk Kunci Enkripsi, pilih AWS KMS Kunci, baik Kunci KMS AWS terkelola yang dibuat oleh Amazon WorkSpaces atau Kunci KMS yang Anda buat. Kunci KMS yang Anda pilih harus simetris. Amazon WorkSpaces tidak mendukung KMS Keys asimetris.
   c. Pilih Langkah Selanjutnya.
4. Pilih Luncurkan WorkSpaces.

Lihat terenkripsi WorkSpaces

Untuk melihat volume WorkSpaces dan mana yang telah dienkripsi dari WorkSpaces konsol, pilih WorkSpacesdari bilah navigasi di sebelah kiri. Kolom Enkripsi Volume menunjukkan apakah masing-masing WorkSpace enkripsi diaktifkan atau dinonaktifkan. Untuk melihat volume spesifik mana yang telah dienkripsi, perluas WorkSpace entri untuk melihat bidang Volume Terenkripsi.

Nyalakan ulang WorkSpace

Kadang-kadang, Anda mungkin perlu me-reboot (restart) secara WorkSpace manual. Mem-boot ulang WorkSpace memutus pengguna dan kemudian melakukan shutdown dan reboot dari file. WorkSpace Untuk menghindari kehilangan data, pastikan pengguna menyimpan dokumen terbuka dan file aplikasi lainnya sebelum Anda me-reboot file WorkSpace. Data pengguna, sistem operasi, dan pengaturan sistem tidak terpengaruh.

> **Warning**
>
> Untuk me-reboot yang dienkripsi WorkSpace, pertama-tama pastikan bahwa AWS KMS Kunci diaktifkan; jika tidak, WorkSpace menjadi tidak dapat digunakan. Untuk menentukan apakah Kunci KMS diaktifkan, lihat Menampilkan Rincian Kunci KMS di Panduan PengembangAWS Key Management Service.

Untuk me-reboot WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih WorkSpaces untuk reboot dan pilih Actions, Reboot WorkSpaces.
4. Saat diminta konfirmasi, pilih Reboot WorkSpaces.

Untuk me-reboot a WorkSpace menggunakan AWS CLI

Gunakan perintah boot ulang-workspaces.

Untuk reboot massal WorkSpaces

Gunakan amazon-workspaces-admin-module.

Membangun kembali WorkSpace

Membangun WorkSpace ulang volume root, volume pengguna, dan antarmuka elastis network utama dari gambar terbaru dari bundel yang WorkSpace diluncurkan. Membangun kembali WorkSpace menghapus lebih banyak data daripada memulihkan WorkSpace, tetapi itu hanya mengharuskan Anda untuk memiliki snapshot dari volume pengguna. Untuk mengembalikan WorkSpace, lihatKembalikan WorkSpace.

Membangun kembali a WorkSpace menyebabkan hal berikut terjadi:

- Volume root (untuk Microsoft Windows, drive C; untuk Linux,/) disegarkan dengan gambar terbaru dari bundel yang WorkSpace dibuat dari. Setiap aplikasi yang diinstal, atau pengaturan sistem yang diubah setelah WorkSpace dibuat, hilang.
- Volume pengguna (untuk Microsoft Windows, drive D; untuk Linux, /home) diciptakan ulang dari snapshot terbaru. Isi saat ini volume pengguna ditimpa.

Snapshot otomatis untuk digunakan saat membangun kembali a WorkSpace dijadwalkan setiap 12 jam. Cuplikan volume pengguna ini diambil terlepas dari kesehatan. WorkSpace Saat Anda memilih Actions, Rebuild /Restore WorkSpace, tanggal dan waktu snapshot terbaru ditampilkan.

- Antarmuka jaringan elastis utama dibuat ulang. WorkSpace Menerima alamat IP pribadi baru.

> **Important**
>
> Setelah 14 Januari 2020, WorkSpaces dibuat dari bundel Windows 7 publik tidak dapat lagi dibangun kembali. Anda mungkin ingin mempertimbangkan untuk memigrasi Windows 7 Anda WorkSpaces ke Windows 10. Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.

Anda dapat membangun kembali WorkSpace hanya jika kondisi berikut terpenuhi:

- WorkSpace Harus memiliki keadaan`AVAILABLE`,,`ERROR`, `UNHEALTHY`atau`STOPPED`, atau`REBOOTING`. Untuk membangun kembali `REBOOTING` status WorkSpace dalam, Anda harus menggunakan operasi RebuildWorkspacesAPI atau perintah AWS CLIrebuild-workspaces.
- Snapshot dari volume pengguna harus ada.

Untuk membangun kembali WorkSpace

> **Warning**
>
> Untuk membangun kembali terenkripsi WorkSpace, pertama-tama pastikan bahwa AWS KMS Kunci diaktifkan; jika tidak, menjadi tidak dapat digunakan. WorkSpace Untuk menentukan apakah Kunci KMS diaktifkan, lihat Menampilkan Rincian Kunci KMS di Panduan PengembangAWS Key Management Service.

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih WorkSpace untuk membangun kembali dan memilih Actions, Rebuild /Restore. WorkSpace
4. Di bawah Snapshot, pilih cap waktu snapshot.
5. Pilih Membangun kembali.

Untuk membangun kembali WorkSpace menggunakan AWS CLI

Gunakan perintah membangun ulang-workspace.

Pemecahan Masalah

Jika Anda membangun kembali WorkSpace setelah mengubah atribut penamaan pengguna SAM AccountName pengguna di Active Directory, Anda mungkin menerima pesan galat berikut:

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

Untuk mengatasi masalah ini, kembalikan ke atribut penamaan pengguna asli dan kemudian memulai kembali pembangunan kembali, atau buat yang baru WorkSpace untuk pengguna tersebut.

Kembalikan WorkSpace

Memulihkan WorkSpace membuat ulang volume root dan volume pengguna, berdasarkan snapshot terbaru dari volume ini yang dibuat saat sehat. WorkSpace Memulihkan data WorkSpace menghapus lebih sedikit data daripada membangun kembali file. WorkSpace Namun, ini mengharuskan Anda untuk memiliki snapshot dari volume root dan volume pengguna, sementara membangun kembali WorkSpace hanya memerlukan snapshot dari volume pengguna. Untuk membangun kembali WorkSpace, lihatMembangun kembali WorkSpace.

Memulihkan WorkSpace penyebab berikut terjadi:

- Volume root (untuk Microsoft Windows, drive C; untuk Linux,/) dipulihkan ke snapshot terbaru. Setiap aplikasi yang diinstal, atau pengaturan sistem yang diubah setelah snapshot terbaru dibuat, akan hilang.
- Volume pengguna (untuk Microsoft Windows, drive D; untuk Linux, /home) diciptakan ulang dari snapshot terbaru. Isi saat ini volume pengguna ditimpa.

Ketika snapshot diambil

Snapshot dari root dan volume pengguna diambil atas dasar berikut. Saat Anda memilih Actions, Rebuild /Restore WorkSpace, tanggal dan waktu snapshot terbaru ditampilkan.

- Setelah a pertama kali WorkSpace dibuat — Biasanya, snapshot awal dari root dan volume pengguna diambil segera setelah WorkSpace dibuat (seringkali dalam 30 menit). Di beberapa AWS

Wilayah, mungkin diperlukan beberapa jam untuk mengambil snapshot awal setelah WorkSpace dibuat.

Jika a WorkSpace menjadi tidak sehat sebelum snapshot awal diambil, tidak WorkSpace dapat dipulihkan. Dalam hal ini, Anda dapat mencoba membangun kembali WorkSpace atau menghubungi AWS Support untuk bantuan.

- Selama penggunaan reguler — Snapshot otomatis untuk digunakan saat memulihkan WorkSpace dijadwalkan setiap 12 jam. Jika sehat, snapshot dari volume root dan volume pengguna dibuat sekitar waktu yang sama. WorkSpace Jika WorkSpace tidak sehat, snapshot dibuat hanya untuk volume pengguna.
- WorkSpace Setelah a dipulihkan — Saat Anda memulihkan WorkSpace, snapshot baru diambil segera setelah pemulihan selesai (seringkali dalam 30 menit). Di beberapa AWS Wilayah, mungkin diperlukan beberapa jam untuk mengambil foto ini setelah WorkSpace dipulihkan.

  Setelah a WorkSpace dipulihkan, jika WorkSpace menjadi tidak sehat sebelum snapshot baru dapat diambil, tidak WorkSpace dapat dipulihkan lagi. Dalam hal ini, Anda dapat mencoba membangun kembali WorkSpace atau menghubungi AWS Support untuk bantuan.

Anda dapat mengembalikan WorkSpace hanya jika kondisi berikut terpenuhi:

- WorkSpace Harus memiliki keadaan`AVAILABLE`,, `ERROR` `UNHEALTHY`, atau`STOPPED`.
- Snapshots root dan volume pengguna harus ada.

Untuk mengembalikan WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih tombol WorkSpace untuk memulihkan dan memilih Actions, Rebuild /Restore WorkSpace.
4. Di bawah Snapshot, pilih stempel waktu snapshot.
5. Pilih Pemulihan.

Untuk mengembalikan WorkSpace menggunakan AWS CLI

Gunakan perintah pulihkan-workspace.

Microsoft 365 Bawa Lisensi Anda Sendiri (BYOL)

Amazon WorkSpaces memungkinkan Anda membawa lisensi Microsoft 365 Anda sendiri jika memenuhi persyaratan lisensi Microsoft. Lisensi ini memungkinkan Anda menginstal dan mengaktifkan Microsoft 365 Apps untuk perangkat lunak perusahaan WorkSpaces yang didukung oleh sistem operasi berikut:

- Windows 10 (Bawa Lisensi Anda Sendiri)
- Windows 11 (Bawa Lisensi Anda Sendiri)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Untuk menggunakan Aplikasi Microsoft 365 untuk perusahaan aktif WorkSpaces, Anda harus berlangganan Microsoft 365 E3/E5, Microsoft 365 A3/A5, atau Microsoft 365 Business Premium.

Di Amazon, WorkSpaces Anda dapat menggunakan lisensi Microsoft 365 untuk menginstal dan mengaktifkan Aplikasi Microsoft 365 untuk perusahaan, termasuk yang berikut ini:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

Untuk informasi selengkapnya, lihat daftar lengkap Aplikasi Microsoft 365 untuk perusahaan.

Anda juga dapat menginstal aplikasi Microsoft yang tidak disertakan dengan Microsoft 365, seperti Microsoft Project, Microsoft Visio, dan Microsoft Power Automate, WorkSpaces tetapi Anda harus membawa lisensi tambahan Anda sendiri.

Anda dapat menginstal dan menggunakan Microsoft 365 dan aplikasi Microsoft lainnya pada primer WorkSpaces dan failover WorkSpaces menggunakan Ketahanan Multi-Wilayah.

Daftar Isi

- Buat WorkSpaces dengan Microsoft 365 Apps untuk perusahaan
- Migrasi yang sudah ada WorkSpaces untuk menggunakan Microsoft 365 Apps for enterprise
- Perbarui Aplikasi Microsoft 365 Anda untuk perusahaan di WorkSpaces

Buat WorkSpaces dengan Microsoft 365 Apps untuk perusahaan

Untuk membuat WorkSpaces dengan Microsoft 365 Apps for enterprise, Anda harus membuat gambar kustom dengan aplikasi yang diinstal, dan menggunakannya untuk membuat bundel kustom. Anda dapat menggunakan bundel untuk meluncurkan WorkSpaces yang baru yang memiliki aplikasi yang diinstal. WorkSpaces tidak menyediakan bundel publik dengan Microsoft 365 Apps for enterprise.

Untuk membuat WorkSpaces dengan Microsoft 365 Apps for enterprise:

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Luncurkan WorkSpace yang ingin Anda gunakan sebagai gambar untuk aplikasi Microsoft lainnya WorkSpaces. Di sinilah Anda akan menginstal aplikasi Microsoft Anda. Untuk informasi selengkapnya tentang meluncurkan WorkSpace, lihat Meluncurkan desktop virtual menggunakan WorkSpaces.
3. Mulai aplikasi klien di https://clients.amazonworkspaces.com/, masukkan kode pendaftaran dari email undangan Anda, dan pilih Daftar.
4. Saat diminta untuk masuk, masukkan kredenal masuk pengguna, lalu pilih Masuk.
5. Instal dan konfigurasikan Aplikasi Microsoft 365 Anda untuk perusahaan.
6. Buat gambar kustom dari WorkSpace, dan gunakan untuk membuat bundel kustom. Untuk informasi selengkapnya tentang membuat gambar dan bundel kustom, lihat Membuat WorkSpaces gambar dan bundel kustom.
7. Luncurkan WorkSpaces menggunakan bundel khusus yang Anda buat. Ini WorkSpaces memiliki Aplikasi Microsoft 365 untuk perusahaan yang diinstal.

Migrasi yang sudah ada WorkSpaces untuk menggunakan Microsoft 365 Apps for enterprise

Jika Anda WorkSpaces tidak memiliki lisensi Microsoft OfficeAWS, Anda dapat menginstal dan mengonfigurasi Aplikasi Microsoft 365 untuk perusahaan di aplikasi Anda WorkSpaces.

Jika WorkSpaces Anda memiliki lisensi Microsoft OfficeAWS, Anda harus terlebih dahulu membatalkan pendaftaran lisensi Microsoft Office Anda sebelum menginstal Microsoft 365 Apps for enterprise.

Important

Menghapus instalasi aplikasi Microsoft Office dari Anda WorkSpaces tidak membatalkan pendaftaran lisensi. Agar tidak dikenakan biaya untuk lisensi Microsoft Office, batalkan pendaftaran Anda dari aplikasi WorkSpaces Microsoft Office AWS dengan melakukan salah satu hal berikut:

- Kelola aplikasi (disarankan) - Anda dapat menghapus instalan Microsoft Office 2016 dan 2019 dari aplikasi Anda WorkSpaces. Untuk informasi selengkapnya, lihat Mengelola aplikasi. Setelah Anda menghapus instalasi, Anda dapat menginstal Microsoft 365 Apps for enterprise di aplikasi Anda WorkSpaces.
- Migrasi a WorkSpace — Anda dapat memigrasikan WorkSpace dari satu bundel ke bundel lainnya sambil mempertahankan data pada volume pengguna.
  - Migrasikan WorkSpaces ke bundel dengan gambar yang tidak memiliki langganan Microsoft Office. Setelah migrasi selesai, Anda dapat menginstal Microsoft 365 Apps for enterprise di aplikasi Anda WorkSpaces.
  - Atau, buat WorkSpaces gambar dan bundel kustom yang sudah memiliki Microsoft 365 Apps for enterprise yang diinstal pada gambar, lalu migrasi Anda WorkSpaces ke bundel kustom baru ini. Setelah migrasi selesai, WorkSpaces pengguna Anda dapat mulai menggunakan Microsoft 365 Apps for enterprise.
  - Untuk informasi selengkapnya tentang cara bermigrasi WorkSpaces, lihat Memigrasi a. WorkSpace

Perbarui Aplikasi Microsoft 365 Anda untuk perusahaan di WorkSpaces

Secara default, Anda WorkSpaces berjalan di Sistem Operasi Microsoft Windows dikonfigurasi untuk menerima pembaruan dari Pembaruan Windows. Namun, pembaruan untuk Aplikasi Microsoft 365 untuk perusahaan tidak tersedia menggunakan Pembaruan Windows. Siapkan pembaruan agar berjalan secara otomatis dari Office CDN, atau gunakan Windows Server Update Services (WSUS) bersama dengan Microsoft Configuration Manager untuk memperbarui Microsoft 365 Apps for enterprise. Untuk informasi selengkapnya, lihat Mengelola pembaruan ke Aplikasi Microsoft 365 dengan Manajer Konfigurasi Microsoft. Untuk mengatur frekuensi pembaruan aplikasi Microsoft

365, tentukan saluran pembaruan dan atur ke Perusahaan Saat Ini atau Bulanan untuk mematuhi kebijakan WorkSpaces lisensi Microsoft 365.

Tingkatkan Windows BYOL WorkSpaces

Pada Windows Bring Your Own License (BYOL) WorkSpaces, Anda dapat meng-upgrade ke versi Windows yang lebih baru menggunakan proses upgrade di tempat. Ikuti petunjuk dalam topik ini sebagai gantinya.

Proses pemutakhiran di tempat hanya berlaku untuk Windows 10 dan 11 WorkSpaces BYOL.

Important

Jangan menjalankan Sysprep pada upgrade. WorkSpace Jika Anda melakukannya, kesalahan yang mencegah Sysprep dari penyelesaian mungkin terjadi. Jika Anda berencana untuk menjalankan Sysprep, lakukan hanya pada WorkSpace yang belum ditingkatkan.

Note

Anda dapat menggunakan proses ini untuk memutakhirkan Windows 10 dan 11 Anda WorkSpaces ke versi yang lebih baru. Namun, proses ini tidak dapat digunakan untuk memutakhirkan Windows 10 Anda WorkSpaces ke Windows 11.

Daftar Isi

Prasyarat

- Jika Anda telah menunda atau menghentikan sementara peningkatan Windows 10 dan 11 dengan menggunakan Kebijakan Grup atau Manajer Konfigurasi Pusat Sistem (SCCM), aktifkan peningkatan sistem operasi untuk Windows 10 dan 11 Anda. WorkSpaces
- Jika WorkSpace ada AutoStop WorkSpace, ubah ke proses pemutakhiran AlwaysOn WorkSpace sebelum di tempat sehingga tidak akan berhenti secara otomatis saat pembaruan sedang diterapkan. Untuk informasi selengkapnya, lihat Mengubah mode berjalan. Jika Anda lebih suka menyimpan WorkSpace set ke AutoStop, ubah AutoStop waktu menjadi tiga jam atau lebih saat peningkatan berlangsung.
- Proses peningkatan di tempat membuat ulang profil pengguna dengan membuat salinan profil khusus bernama Pengguna Default (`C:\Users\Default`). Jangan gunakan profil pengguna default ini untuk membuat penyesuaian. Kami merekomendasikan membuat penyesuaian untuk profil pengguna melalui objek kebijakan grup (GPO) sebagai gantinya. Penyesuaian dilakukan melalui GPO yang dapat dengan mudah diubah atau digulir kembali dan kurang rentan terhadap kesalahan.
- Proses peningkatan di tempat hanya dapat mencadangkan dan membuat ulang satu profil pengguna. Jika Anda memiliki beberapa profil pengguna di drive D, hapus semua profil kecuali yang Anda butuhkan.

Pertimbangan

Proses pemutakhiran di tempat menggunakan dua skrip registri (`enable-inplace-upgrade.ps1`dan`update-pvdrivers.ps1`) untuk membuat perubahan yang diperlukan pada Anda WorkSpaces yang memungkinkan proses Pembaruan Windows berjalan. Perubahan ini melibatkan pembuatan profil pengguna (sementara) di drive C, bukan di drive D. Jika profil pengguna sudah ada di drive D, data di profil pengguna asli tersebut tetap ada di drive D.

Secara default, WorkSpaces membuat profil pengguna di`D:\Users\%USERNAME%`. Skrip `enable-inplace-upgrade.ps1` mengonfigurasi Windows untuk membuat profil pengguna baru pada `C:\Users\%USERNAME%` dan mengarahkan ulang folder shell pengguna ke `D:\Users\%USERNAME%`. Profil pengguna baru ini dibuat ketika pengguna log pada pertama kalinya.

Setelah peningkatan di tempat, Anda memiliki pilihan untuk meninggalkan profil pengguna Anda di drive C agar pengguna Anda dapat menggunakan proses Pembaruan Windows untuk meningkatkan mesin mereka di masa mendatang. Namun, ketahuilah bahwa WorkSpaces dengan

profil yang disimpan di drive C tidak dapat dibangun kembali atau dimigrasi tanpa kehilangan semua data di profil pengguna kecuali Anda membuat cadangan dan memulihkan data itu sendiri. Jika Anda memutuskan untuk meninggalkan profil pada drive C, Anda dapat menggunakan kunci UserShellFoldersRedirectionregistri untuk mengarahkan folder shell pengguna ke drive D, seperti yang dijelaskan nanti dalam topik ini.

Untuk memastikan bahwa Anda dapat membangun kembali atau memigrasi Anda WorkSpaces dan untuk menghindari potensi masalah dengan pengalihan folder shell pengguna, kami sarankan Anda memilih untuk mengembalikan profil pengguna Anda ke drive D setelah peningkatan di tempat. Anda dapat melakukannya dengan menggunakan kunci registri PostUpgradeRestoreProfileOnD, seperti yang dijelaskan nanti dalam topik ini.

Keterbatasan yang Sudah Diketahui

- Perubahan lokasi profil pengguna dari drive D ke drive C tidak terjadi selama WorkSpace pembangunan kembali atau migrasi. Jika Anda melakukan peningkatan di tempat pada Windows 10 atau 11 BYOL WorkSpace dan kemudian membangun kembali atau memigrasinya, yang baru WorkSpace akan memiliki profil pengguna di drive D.

  > **Warning**
  >
  > Jika Anda meninggalkan profil pengguna di drive C setelah peningkatan di tempat, data profil pengguna yang disimpan di drive C akan hilang selama pembuatan ulang atau migrasi kecuali jika Anda mencadangkan data profil pengguna secara manual sebelum membuat ulang atau bermigrasi, lalu memulihkan secara manual data profil pengguna setelah menjalankan proses pembangunan ulang atau migrasi.

- Jika bundel BYOL default Anda berisi gambar yang didasarkan pada rilis Windows 10 dan 11 sebelumnya, Anda harus melakukan pemutakhiran di tempat lagi setelah dibangun kembali atau WorkSpace dimigrasikan.

Ringkasan pengaturan kunci registri

Untuk mengaktifkan proses pemutakhiran di tempat dan untuk menentukan di mana Anda ingin profil pengguna berada setelah pemutakhiran, Anda harus mengatur sejumlah kunci registri.

Jalur registri: HKL M:\Software\Amazon\WorkSpacesConfig\ enable-inplace-upgrade .ps1

Kunci registri	Tipe	Nilai
Diaktifkan	DWORD	0 – (Default) Menonaktifkan peningkatan di tempat 1 – Mengaktifkan peningkatan di tempat
PostUpgradeRestoreProfileOnD	DWORD	0 – (Default) Tidak mencoba memulihkan jalur profil pengguna setelah peningkatan di tempat 1 - Mengembalikan jalur profil pengguna (ProfileImagePath) setelah peningkatan di tempat
UserShellFoldersRedirection	DWORD	0 – Tidak mengaktifkan pengalihan folder shell pengguna 1 – (Default) Mengaktifkan pengalihan folder shell pengguna ke `D:\Users\%USERNAME%` setelah profil pengguna diregenerasi pada `C:\Users\%USERNAME%`
NoReboot	DWORD	0 – (Default) Mengizinkan Anda untuk mengontrol ketika boot ulang terjadi setelah mengubah registri untuk profil pengguna 1 - Tidak mengizinkan skrip untuk reboot WorkSpace

Kunci registri	Tipe	Nilai
		setelah memodifikasi registri untuk profil pengguna

Jalur registri: HKL M:\Software\Amazon\WorkSpacesConfig\ update-pvdrivers.ps1

Kunci registri	Tipe	Nilai
Diaktifkan	DWORD	0 - (Default) Menonaktifkan pembaruan driver AWS PV 1 - Mengaktifkan pembaruan driver AWS PV

Lakukan pemutakhiran langsung

Untuk mengaktifkan upgrade Windows di tempat pada BYOL Anda WorkSpaces, Anda harus mengatur kunci registri tertentu, seperti yang dijelaskan dalam prosedur berikut. Anda juga harus mengatur kunci registri tertentu untuk menunjukkan drive (C atau D) di mana Anda ingin profil pengguna berada setelah upgrade di tempat selesai.

Anda dapat membuat perubahan registri ini secara manual. Jika Anda memiliki beberapa WorkSpaces untuk diperbarui, Anda dapat menggunakan Kebijakan Grup atau SCCM untuk mendorong skrip. PowerShell Untuk contoh PowerShell skrip, lihatPerbarui WorkSpace registri Anda menggunakan PowerShell skrip.

Untuk melakukan pemutakhiran Windows 10 dan 11 di tempat

1. Catat versi Windows mana yang saat ini berjalan di Windows 10 dan 11 BYOL WorkSpaces yang Anda perbarui, lalu reboot.
2. Perbarui kunci registri sistem Windows berikut untuk mengubah data nilai untuk Diaktifkan dari 0 ke 1. Perubahan registri ini memungkinkan peningkatan di tempat untuk file. WorkSpace

   - HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade
   - HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Amazon\\ update-pvdrivers.ps1 WorkSpacesConfig

> **Note**
>
> Jika kunci ini tidak ada, reboot tombol WorkSpace. Kunci harus ditambahkan saat sistem di-boot ulang.

(Opsional) Jika Anda menggunakan alur kerja terkelola seperti urutan tugas SCCM untuk melakukan peningkatan, tetapkan nilai kunci berikut ke 1 untuk mencegah komputer dari boot ulang:

HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade NoReboot

3. Tentukan drive mana yang ingin Anda gunakan untuk profil pengguna setelah proses peningkatan di tempat (untuk informasi selengkapnya, lihatPertimbangan), dan atur kunci registri sebagai berikut:

   - Pengaturan jika Anda ingin profil pengguna pada drive C setelah peningkatan:

     HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     Nama kunci: PostUpgradeRestoreProfileOnD

     Nilai kunci: 0

     Nama kunci: UserShellFoldersRedirection

     Nilai kunci: 1

   - Pengaturan jika Anda ingin profil pengguna pada drive C setelah peningkatan:

     HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     Nama kunci: PostUpgradeRestoreProfileOnD

     Nilai kunci: 1

Nama kunci: UserShellFoldersRedirection

Nilai kunci: 0

4. Setelah menyimpan perubahan ke registri, reboot WorkSpace lagi sehingga perubahan diterapkan.

> **Note**
>
> - Setelah reboot, masuk ke WorkSpace membuat profil pengguna baru. Anda mungkin melihat ikon placeholder di menu mulai. Perilaku ini secara otomatis diselesaikan setelah peningkatan di tempat selesai.
> - Biarkan 10 menit untuk memastikan bahwa tidak WorkSpace diblokir.

(Opsional) Konfirmasikan bahwa nilai kunci berikut diatur ke 1, yang membuka blokir WorkSpace untuk memperbarui:

HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Amazon\\ .ps1\ Dihapus WorkSpacesConfig enable-inplace-upgrade profileImagePath

5. Lakukan peningkatan di tempat. Anda dapat menggunakan metode mana pun yang Anda suka, seperti SCCM, ISO, atau Windows Update (WU). Bergantung pada versi Windows 10 dan 11 asli Anda dan berapa banyak aplikasi yang diinstal, proses ini dapat memakan waktu 40 hingga 120 menit.

> **Note**
>
> Proses peningkatan di tempat mungkin memakan waktu setidaknya satu jam. Status WorkSpace instans mungkin muncul seperti `UNHEALTHY` selama peningkatan.

6. Setelah proses pembaruan selesai, konfirmasi bahwa versi Windows telah diperbarui.

> **Note**
>
> Jika pemutakhiran di tempat gagal, Windows secara otomatis memutar kembali untuk menggunakan versi Windows 10 dan 11 yang ada sebelum Anda memulai

pemutakhiran. Untuk informasi selengkapnya tentang pemecahan masalah, lihat Dokumentasi Microsoft.

(Opsional) Untuk mengonfirmasi bahwa skrip pembaruan telah berhasil dijalankan, verifikasi bahwa nilai kunci berikut diatur ke 1:

HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. Jika Anda memodifikasi mode berjalan WorkSpace dengan menyetelnya ke AlwaysOn atau dengan mengubah periode AutoStop waktu sehingga proses pemutakhiran di tempat dapat berjalan tanpa gangguan, atur mode berjalan kembali ke pengaturan awal Anda. Untuk informasi selengkapnya, lihat Mengubah mode berjalan.

Jika Anda belum menyetel kunci registri PostUpgradeRestoreProfileOnD ke 1, profil pengguna dibuat ulang oleh Windows dan ditempatkan `C:\Users\%USERNAME%` setelah peningkatan di tempat, sehingga Anda tidak perlu melalui langkah-langkah di atas lagi untuk upgrade Windows 10 dan 11 di tempat yang akan datang. Secara default, pengalihan skrip `enable-inplace-upgrade.ps1` folder shell berikut untuk drive D:

- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu`

- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates`

Jika Anda mengarahkan folder shell ke lokasi lain di lokasi Anda WorkSpaces, lakukan operasi yang diperlukan WorkSpaces setelah peningkatan di tempat.

Pemecahan Masalah

Jika Anda mengalami masalah dengan pembaruan, Anda dapat memeriksa item berikut untuk membantu pemecahan masalah:

- Log Windows, yang terletak, secara default, di lokasi-lokasi berikut:

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\`

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED`
- Penampil Peristiwa Windows

  Windows Log > Aplikasi> Sumber: Amazon WorkSpaces

> **Tip**
>
> Selama proses peningkatan di tempat, jika Anda melihat bahwa beberapa pintasan ikon di desktop tidak lagi berfungsi, itu karena WorkSpaces memindahkan profil pengguna apa pun yang terletak di drive D ke drive C untuk mempersiapkan peningkatan. Setelah peningkatan selesai, pintasan akan bekerja seperti yang diharapkan.

Perbarui WorkSpace registri Anda menggunakan PowerShell skrip

Anda dapat menggunakan PowerShell skrip contoh berikut untuk memperbarui registri pada Anda WorkSpaces untuk mengaktifkan peningkatan di tempat. IkutiLakukan pemutakhiran langsung, tetapi gunakan skrip ini untuk memperbarui registri pada masing-masing WorkSpace.

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
```

```
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

Migrasi a WorkSpace

> **Note**
>
> Jika Anda ingin berhenti berlangganan atau menghapus lisensi versi Microsoft Office AWS dari Anda WorkSpace, sebaiknya gunakan Kelola aplikasi.

Anda dapat memigrasikan WorkSpace dari satu bundel ke bundel lainnya, sambil mempertahankan data pada volume pengguna. Berikut ini adalah contoh skenario:

- Anda dapat bermigrasi WorkSpaces dari pengalaman desktop Windows 7 ke pengalaman desktop Windows 10.
- Anda dapat bermigrasi WorkSpaces dari protokol PCoIP ke Protokol WorkSpaces Streaming (WSP).
- Anda dapat bermigrasi WorkSpaces dari Microsoft Office 32-bit pada bundel yang didukung Windows Server 2016 ke Microsoft Office 64-bit di Windows Server 2019 dan WorkSpaces bundel yang didukung Windows Server 2022. WorkSpaces
- Anda dapat bermigrasi WorkSpaces dari satu bundel publik atau kustom ke bundel lainnya. Misalnya, Anda dapat bermigrasi dari GPU-enabled (Graphics.g4dn. GraphicsPro.g4dn, Graphics, and GraphicsPro) bundel ke bundel non-GPU, serta ke arah lain.
- Anda dapat bermigrasi WorkSpaces dari Windows 10 BYOL ke Windows 11 BYOL tetapi migrasi dari Windows 11 ke Windows 10 tidak didukung.
- Paket nilai tidak didukung di Windows 11. Untuk memigrasikan paket nilai Windows 7 atau 10 Anda WorkSpaces ke Windows 11, Anda perlu mengalihkan Nilai WorkSpaces Anda ke penawaran bundel yang lebih besar terlebih dahulu.
- Sebelum bermigrasi WorkSpaces dari Windows 7 ke Windows 11, Anda harus memigrasikannya ke Windows 10. Masuk ke Windows 10 WorkSpace setidaknya sekali sebelum memigrasikannya ke Windows 11. Migrasi dari Windows 7 WorkSpaces langsung ke Windows 11 tidak didukung.
- Anda dapat memigrasikan Windows WorkSpaces yang menggunakan Microsoft Office melalui AWS WorkSpaces paket kustom dengan aplikasi Microsoft 365. Setelah migrasi, Anda berhenti WorkSpaces berlangganan dari Microsoft Office.
- Anda dapat memigrasikan Windows WorkSpaces yang menggunakan Microsoft Office AWS ke WorkSpaces bundel tanpa langganan Office 2016/2019. Setelah migrasi, Anda berhenti WorkSpaces berlangganan dari Microsoft Office.

Untuk informasi selengkapnya tentang WorkSpaces bundel Amazon, lihatWorkSpace bundel dan gambar.

Proses migrasi membuat ulang WorkSpace dengan menggunakan volume root baru dari gambar bundel target dan volume pengguna dari snapshot terakhir yang tersedia dari aslinya. WorkSpace Profil pengguna baru dibuat selama migrasi untuk kompatibilitas yang lebih baik. Profil pengguna lama diganti nama, lalu file tertentu di profil pengguna lama dipindahkan ke profil pengguna baru. (Untuk detail tentang apa yang akan dipindahkan, lihat Apa yang terjadi selama migrasi.)

Proses migrasi memakan waktu hingga satu jam per WorkSpace. Saat Anda memulai proses migrasi, yang baru akan WorkSpace dibuat. Jika terjadi kesalahan yang mencegah migrasi berhasil, aslinya WorkSpace dipulihkan dan dikembalikan ke keadaan semula, dan yang baru WorkSpace dihentikan.

Daftar Isi

Batas migrasi

- Anda tidak dapat bermigrasi ke paket pengalaman desktop Windows 7 publik atau kustom. Anda juga tidak dapat memigrasi untuk membawa Anda sendiri lisensi (BYOL) Windows 7 paket.
- Anda dapat memigrasikan BYOL WorkSpaces hanya ke bundel BYOL lainnya. Untuk memigrasikan BYOL WorkSpace dari PCoIP ke WSP, Anda harus terlebih dahulu membuat bundel BYOL dengan protokol WSP. Anda kemudian dapat memigrasikan PCoIP BYOL Anda WorkSpaces ke bundel WSP BYOL itu.
- Anda tidak dapat memigrasikan yang WorkSpace dibuat dari bundel publik atau kustom ke bundel BYOL.
- Graphics.g4dn, GraphicsPro .g4dn, Graphics, dan GraphicsPro bundel hanya tersedia untuk protokol PCoIP saat ini, jadi Graphics.g4dn, .g4dn, Graphics, dan belum dapat dimigrasikan ke WSP. GraphicsPro GraphicsPro WorkSpaces

- Migrasi Linux saat WorkSpaces ini tidak didukung.
- Di AWS Wilayah yang mendukung lebih dari satu bahasa, Anda dapat bermigrasi WorkSpaces antar bundel bahasa.
- Sumber dan target paket harus berbeda. (Namun, di Wilayah yang mendukung lebih dari satu bahasa, Anda dapat bermigrasi ke paket Windows 10 yang sama selama bahasanya berbeda.) Jika Anda ingin menyegarkan WorkSpace menggunakan bundel yang sama, buat kembali WorkSpace sebagai gantinya.
- Anda tidak dapat bermigrasi WorkSpaces di seluruh Wilayah.
- Dalam beberapa kasus, jika migrasi tidak berhasil diselesaikan, Anda mungkin tidak menerima pesan kesalahan, dan mungkin tampak bahwa proses migrasi tidak dimulai. Jika WorkSpace bundel tetap sama satu jam setelah mencoba migrasi, migrasi tidak berhasil. Hubungi Pusat AWS Support untuk mendapatkan bantuan.

Skenario migrasi

Tabel berikut menunjukkan skenario migrasi mana yang tersedia:

OS Sumber	OS Target	Tersedia?
Paket publik atau kustom Windows 7	Paket publik atau kustom Windows 10	Ya
Paket kustom Windows 7	Paket publik Windows 7	Tidak
Paket kustom Windows 7	Paket kustom Windows 7	Tidak
Paket publik Windows 7	Paket kustom Windows 7	Tidak
Paket publik atau kustom Windows 10	Paket publik atau kustom Windows 7	Tidak
Paket publik atau kustom Windows 10	Paket kustom Windows 10	Ya
Paket BYOL Windows 7	Paket BYOL Windows 7	Tidak
Paket BYOL Windows 7	Paket BYOL Windows 10	Ya

OS Sumber	OS Target	Tersedia?
Paket BYOL Windows 10	Paket BYOL Windows 7	Tidak
Paket BYOL Windows 10	Paket BYOL Windows 10	Ya
Bundel Windows 10 Publik yang didukung Windows Server 2016	Bundel Windows 10 Publik yang didukung Windows Server 2019 	Ya
Bundel Windows 10 Publik yang didukung Windows Server 2019 	Bundel Windows 10 Publik yang didukung Windows Server 2016	Ya
Paket BYOL Windows 10	Bundel Windows 11 BYOL	Ya
Bundel Windows 11 BYOL	Paket BYOL Windows 10	Tidak
Bundel Windows 10 kustom yang didukung Windows Server 2016	Bundel Windows 10 Publik yang didukung Windows Server 2019	Ya
Bundel Windows 10 kustom yang didukung Windows Server 2016	Bundel Windows 10 Publik yang didukung Windows Server 2022	Ya
Bundel Windows 10 kustom yang didukung Windows Server 2019	Bundel Windows 10 Publik yang didukung Windows Server 2022	Ya

> **Note**
>
> Akses web tidak tersedia untuk cabang PCoIP bundel Windows 10 Public Windows 10 yang didukung Windows Server 2019.

> **Important**
>
> Bundel Windows 10 plus Public Server 2016 yang didukung Windows Server mencakup Microsoft Office 2016 dan Layanan Keamanan Bisnis Bebas Khawatir Trend Micro. Bundel Public Windows 10 plus yang didukung Windows Server 2019 hanya mencakup Microsoft Office 2019, dan tidak termasuk Layanan Trend Micro.

Apa yang terjadi selama migrasi

Selama migrasi, data pada volume pengguna (drive D) dipertahankan, tetapi semua data pada volume root (drive C) hilang. Ini berarti bahwa tidak ada aplikasi yang diinstal, pengaturan, dan perubahan pada registri yang dipertahankan. Folder profil pengguna lama berganti nama dengan sufiks `.NotMigrated`, dan profil pengguna baru dibuat.

Proses migrasi membuat ulang drive D berdasarkan snapshot terakhir dari volume pengguna asli. Selama boot pertama yang baru WorkSpace, proses migrasi memindahkan `D:\Users\%USERNAME%` folder asli ke folder bernama`D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. Folder `D:\Users\%USERNAME%\` baru dibuat oleh OS baru.

Setelah profil pengguna baru dibuat, file dalam folder shell pengguna berikut dipindahkan dari profil `.NotMigrated` ke profil baru:

- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`

Important

Proses migrasi mencoba untuk memindahkan file dari profil pengguna lama ke profil baru. Berkas apa pun yang tidak dipindahkan selama migrasi tetap berada di folder `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. Jika migrasi berhasil, Anda dapat melihat file mana yang dipindahkan ke `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. Anda dapat secara manual memindahkan file apa pun yang tidak dipindahkan secara otomatis.

Secara default, paket publik memiliki pengindeksan pencarian lokal yang dinonaktifkan. Jika Anda mengaktifkannya, default-nya adalah untuk mencari `C:\Users` dan bukan `D:\Users`, jadi Anda perlu menyesuaikannya juga. Jika Anda telah menetapkan pengindeksan pencarian lokal secara khusus ke `D:\Users\`*`username`* dan bukan ke `D:\Users`, maka pengindeksan pencarian lokal mungkin tidak bekerja pasca-migrasi untuk setiap berkas pengguna yang berada di folder `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`.

Setiap tag yang ditetapkan ke aslinya WorkSpace dibawa selama migrasi, dan mode berjalan WorkSpace dipertahankan. Namun, yang baru WorkSpace mendapat WorkSpace ID baru, nama komputer, dan alamat IP.

Praktik terbaik

Sebelum Anda memigrasikan a WorkSpace, lakukan hal berikut:

- Cadangkan data penting apa pun pada drive C ke lokasi lain. Semua data pada drive C dihapus selama migrasi.
- Pastikan bahwa migrasi setidaknya berusia 12 jam, untuk memastikan bahwa snapshot volume pengguna telah dibuat. WorkSpace Pada WorkSpaces halaman Migrasi di WorkSpaces konsol Amazon, Anda dapat melihat waktu snapshot terakhir. Setiap data yang dibuat setelah snapshot terakhir hilang selama migrasi.
- Untuk menghindari potensi kehilangan data, pastikan pengguna Anda keluar dari mereka WorkSpaces dan tidak masuk kembali sampai setelah proses migrasi selesai. Perhatikan bahwa WorkSpaces tidak dapat dimigrasikan saat berada dalam `ADMIN_MAINTENANCE` mode.
- Pastikan bahwa WorkSpaces Anda ingin bermigrasi memiliki status`AVAILABLE`,`STOPPED`, atau`ERROR`.

- Pastikan bahwa Anda memiliki cukup alamat IP untuk WorkSpaces Anda bermigrasi. Selama migrasi, alamat IP baru akan dialokasikan untuk file. WorkSpaces
- Jika Anda menggunakan skrip untuk bermigrasi WorkSpaces, migrasikan dalam batch tidak lebih dari 25 WorkSpaces sekaligus.

Memecahkan masalah

- Jika pengguna Anda melaporkan file yang hilang setelah migrasi, periksa untuk melihat apakah file profil pengguna mereka tidak dipindahkan selama proses migrasi. Anda dapat melihat file mana yang dipindahkan `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. File-file yang tidak dipindahkan akan ditempatkan di folder `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. Anda dapat secara manual memindahkan file apa pun yang tidak dipindahkan secara otomatis.
- Jika Anda menggunakan API untuk bermigrasi WorkSpaces dan migrasi tidak berhasil, WorkSpace ID target yang dikembalikan oleh API tidak akan digunakan, dan masih WorkSpace akan memiliki WorkSpace ID asli.
- Jika migrasi tidak berhasil selesai, periksa Direktori Aktif untuk melihat apakah itu dibersihkan sesuai. Anda mungkin perlu menghapus secara manual WorkSpaces yang tidak lagi Anda butuhkan.

Bagaimana penagihan terpengaruh

Selama bulan di mana migrasi terjadi, Anda akan dikenakan jumlah prorata untuk yang baru dan yang asli. WorkSpaces Misalnya, jika Anda bermigrasi WorkSpace A ke WorkSpace B pada 10 Mei, Anda akan dikenakan biaya WorkSpace A dari 1 Mei hingga 10 Mei, dan Anda akan dikenakan biaya untuk WorkSpace B mulai 11 Mei hingga 30 Mei.

> **Note**
>
> Jika Anda memigrasikan WorkSpace ke jenis bundel yang berbeda (misalnya, dari Kinerja ke Daya, atau Nilai ke Standar), ukuran volume root (drive C) dan volume pengguna (drive D) mungkin meningkat selama proses migrasi. Jika perlu, volume root meningkat untuk mencocokkan ukuran volume root default untuk paket baru. Namun, jika Anda telah menentukan ukuran yang berbeda (lebih tinggi atau lebih rendah) untuk volume pengguna daripada default untuk paket asli, ukuran volume pengguna yang sama akan dipertahankan

selama proses migrasi. Jika tidak, proses migrasi menggunakan ukuran volume WorkSpace pengguna sumber yang lebih besar dan ukuran volume pengguna default untuk bundel baru.

Migrasi a WorkSpace

Anda dapat bermigrasi WorkSpaces melalui WorkSpaces konsol Amazon, AWS CLI atau Amazon WorkSpaces API.

Untuk memigrasikan a WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih WorkSpace dan pilih Tindakan, Migrasi. WorkSpaces
4. Di bawah Bundel, pilih bundel yang ingin Anda WorkSpace migrasi.

   > **Note**
   >
   > Untuk memigrasikan BYOL WorkSpace dari PCoIP ke WSP, Anda harus terlebih dahulu membuat bundel BYOL dengan protokol WSP. Anda kemudian dapat memigrasikan PCoIP BYOL Anda WorkSpaces ke bundel WSP BYOL itu.

5. Pilih Migrasi. WorkSpaces

   Yang baru WorkSpace dengan status `PENDING` muncul di WorkSpaces konsol Amazon. Ketika migrasi selesai, aslinya akan WorkSpace dihentikan, dan status baru WorkSpace disetel ke`AVAILABLE`.

6. (Opsional) Untuk menghapus setiap paket kustom dan citra yang tidak Anda perlukan lagi, lihat Hapus WorkSpaces bundel atau gambar khusus.

Untuk bermigrasi WorkSpaces melaluiAWS CLI, gunakan perintah migrate-workspace. Untuk bermigrasi WorkSpaces melalui Amazon WorkSpaces API, lihat MigrateWorkSpacedi Referensi Amazon WorkSpaces API.

Menghapus WorkSpace

Setelah selesai dengan a WorkSpace, Anda dapat menghapusnya. Anda juga dapat menghapus sumber daya terkait.

> **Warning**
>
> Menghapus a WorkSpace adalah tindakan permanen dan tidak dapat dibatalkan. Data WorkSpace pengguna tidak bertahan dan dihancurkan. Untuk bantuan dengan mencadangkan data pengguna, hubungi AWS Support.

> **Note**
>
> Simple AD dan AD Connector tersedia untuk Anda secara gratis untuk digunakan WorkSpaces. Jika tidak ada yang WorkSpaces digunakan dengan direktori Simple AD atau AD Connector selama 30 hari berturut-turut, direktori ini akan secara otomatis dideregistrasi untuk digunakan dengan Amazon WorkSpaces, dan Anda akan dikenakan biaya untuk direktori ini sesuai ketentuan harga. AWS Directory Service
> Untuk menghapus direktori kosong, lihat Hapus direktori untuk WorkSpaces. Jika Anda menghapus direktori Simple AD atau AD Connector, Anda selalu dapat membuat yang baru ketika Anda ingin mulai menggunakan WorkSpaces lagi.

Untuk menghapus WorkSpace

Anda dapat menghapus WorkSpace yang ada di negara bagian mana pun kecuali Ditangguhkan.

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih Anda WorkSpace dan pilih Hapus.
4. Saat diminta konfirmasi, pilih Delete WorkSpace (Hapus). Dibutuhkan sekitar 5 menit untuk menghapus file WorkSpace. Selama penghapusan, status diatur ke WorkSpace Terminating. Ketika penghapusan selesai, WorkSpace menghilang dari konsol.
5. (Opsional) Untuk menghapus semua paket kustom dan citra yang telah Anda selesaikan, lihat Hapus WorkSpaces bundel atau gambar khusus.

6. (Opsional) Setelah Anda menghapus semua WorkSpaces dalam direktori, Anda dapat menghapus direktori. Untuk informasi selengkapnya, lihat Hapus direktori untuk WorkSpaces.
7. (Opsional) Setelah Anda menghapus semua sumber daya di virtual private cloud (VPC) untuk direktori Anda, Anda dapat menghapus VPC dan melepaskan alamat IP elastis yang digunakan untuk gateway NAT. Untuk informasi selengkapnya, lihat Menghapus VPC Anda dan Bekerja dengan alamat IP Elastis dalam Panduan Pengguna Amazon VPC.

Untuk menghapus WorkSpace menggunakan AWS CLI

Gunakan perintah akhiri-workspaces.

WorkSpace bundel dan gambar

WorkSpace Bundel adalah kombinasi dari sistem operasi, dan penyimpanan, komputasi, dan sumber daya perangkat lunak. Saat Anda meluncurkan WorkSpace, Anda memilih bundel yang memenuhi kebutuhan Anda. Bundel default yang tersedia untuk WorkSpaces disebut bundel publik. Untuk informasi selengkapnya tentang berbagai bundel publik yang tersedia WorkSpaces, lihat Amazon WorkSpaces Bundles.

Jika Anda telah meluncurkan Windows atau Linux WorkSpace dan telah menyesuaikannya, Anda dapat membuat gambar khusus dari itu WorkSpace.

Gambar khusus hanya berisi OS, perangkat lunak, dan pengaturan untuk file WorkSpace. Bundel kustom adalah kombinasi dari gambar kustom dan perangkat keras dari mana a WorkSpace dapat diluncurkan.

Setelah membuat gambar kustom, Anda dapat membuat bundel kustom yang menggabungkan WorkSpace gambar kustom dan konfigurasi komputasi dan penyimpanan yang mendasari yang Anda pilih. Anda kemudian dapat menentukan bundel kustom ini ketika Anda meluncurkan baru WorkSpaces untuk memastikan bahwa yang baru WorkSpaces memiliki konfigurasi konsisten yang sama (perangkat keras dan perangkat lunak).

Jika Anda perlu melakukan pembaruan perangkat lunak atau menginstal perangkat lunak tambahan pada Anda WorkSpaces, Anda dapat memperbarui bundel kustom Anda dan menggunakannya untuk membangun kembali Anda WorkSpaces.

WorkSpaces mendukung beberapa sistem operasi (OS) yang berbeda, protokol streaming, dan bundel. Tabel berikut memberikan informasi tentang lisensi, protokol streaming, dan bundel yang didukung oleh masing-masing OS.

Sistem Operasi	Lisensi	Protokol streaming	Bundel yang didukung	Kebijakan siklus hidup/ tanggal pensiun
Windows Server 2016	Termasuk	WSP, PCoIP	Nilai, Standar, Kinerja, Daya,, Grafik (usang) PowerPro,,	Januari 12, 2027

Sistem Operasi	Lisensi	Protokol streaming	Bundel yang didukung	Kebijakan siklus hidup/ tanggal pensiun
			Graphics.g4dn GraphicsPro, .g4dn GraphicsPro	
Windows Server 2019	Termasuk	WSP, PCoIP	Nilai, Standar, Kinerja, Daya,, Grafik (usang) PowerPro,, Graphics.g4dn GraphicsPro, .g4dn GraphicsPro	Januari 9, 2029
Windows Server 2022	Termasuk	WSP, PCoIP	Standar, Kinerja, Daya,, Grafik (usang) PowerPro,, Graphics.g4dn GraphicsPro, .g4dn GraphicsPro	14 Oktober 2031
Windows 10	Bawa Lisensi Sendiri (BYOL)	WSP, PCoIP	Nilai, Standar, Kinerja, Daya,, Grafik (usang) PowerPro,, Graphics.g4dn GraphicsPro, .g4dn GraphicsPro	Dalam mendukung
Windows 11	Bawa Lisensi Sendiri (BYOL)	WSP	Standar, Kinerja, Daya, PowerPro	Dalam mendukung
Amazon Linux 2	Termasuk	WSP, PCoIP	Nilai, Standar, Kinerja, Daya, PowerPro	Juni 30, 2025
Ubuntu 22.04 LTS	Termasuk	WSP	Nilai, Standar, Kinerja, Daya,, PowerPro Grafik.g4dn, .g4dn GraphicsPro	Juni, 2032

> **Note**
>
> - Versi sistem operasi yang tidak lagi didukung oleh vendor tidak dijamin berfungsi dan tidak didukung oleh AWS dukungan.
> - Untuk WorkSpaces berjalan pada sistem operasi Windows, bundel grafis hanya mendukung protokol streaming PCoIP.

Konten

Opsi bundel

Sebelum memilih bundel, pastikan bundel yang ingin Anda pilih kompatibel dengan WorkSpaces 'protokol, sistem operasi, jaringan, dan jenis komputasi Anda. Untuk informasi selengkapnya tentang protokol, lihat Protokol untuk Amazon. WorkSpaces Untuk informasi selengkapnya tentang jaringan, lihat persyaratan jaringan WorkSpaces klien Amazon.

> **Note**
>
> - Kami merekomendasikan untuk tidak melebihi latensi jaringan maksimum 250 ms untuk PCoIP. WorkSpaces Untuk mendapatkan pengalaman WorkSpaces pengguna PCoIP terbaik, kami sarankan untuk menjaga latensi jaringan di bawah 100 ms. Ketika waktu pulang-pergi (RTT) melebihi 375 ms, koneksi WorkSpaces klien akan dimatikan. Untuk pengalaman pengguna WorkSpaces Streaming Protocol (WSP) terbaik, kami sarankan untuk menjaga RTT di bawah 250 ms. Jika RTT antara 250 ms dan 400 ms, pengguna dapat mengakses WorkSpace, tetapi kinerja akan menurun secara signifikan.

- Sebaiknya uji kinerja bundel yang ingin Anda pilih di lingkungan pengujian dengan menjalankan dan menggunakan aplikasi yang mereplikasi tugas harian pengguna Anda.

Important

- Bundel Grafis tidak akan lagi didukung setelah 30 November 2023. Sebaiknya beralih ke bundel Graphics.g4dn untuk menggunakan bundel Grafis. WorkSpaces
- Grafik dan GraphicsPro bundel saat ini tidak tersedia di Wilayah Asia Pasifik (Mumbai).

Berikut ini adalah bundel yang WorkSpaces menawarkan. Untuk informasi tentang bundel di WorkSpaces, lihat Amazon WorkSpaces Bundles.

Bundel nilai

Bundel ini sangat cocok untuk yang berikut:

- Pengeditan teks dasar dan entri data
- Penjelajahan web dengan penggunaan ringan
- Pesan instan

Bundel ini tidak direkomendasikan untuk pengolah kata, konferensi audio dan video, berbagi layar, alat pengembangan perangkat lunak, aplikasi intelijen bisnis, dan aplikasi grafis.

Bundel standar

Bundel ini sangat cocok untuk yang berikut:

- Pengeditan teks dasar dan entri data
- Penjelajahan web
- Pesan instan
- Email

Bundel ini tidak direkomendasikan untuk konferensi audio dan video, berbagi layar, pengolah kata, alat pengembangan perangkat lunak, aplikasi intelijen bisnis, dan aplikasi grafis

Bundel kinerja

Bundel ini sangat cocok untuk yang berikut:

- Penjelajahan web
- Pengolah kata
- Pesan instan
- Email
- Spreadsheet
- Pemrosesan audio
- Courseware

Bundel ini tidak direkomendasikan untuk konferensi video, berbagi layar, alat pengembangan perangkat lunak, aplikasi intelijen bisnis, dan aplikasi grafis

Bundel daya

Bundel ini sangat cocok untuk yang berikut:

- Penjelajahan web
- Pengolah kata
- Email
- Pesan instan
- Spreadsheet
- Pemrosesan audio
- Pengembangan perangkat lunak (Integrated Development Environment (IDE))
- Masuk ke pemrosesan data tingkat menengah
- Konferensi audio dan video

Bundel ini tidak direkomendasikan untuk berbagi layar, alat pengembangan perangkat lunak, aplikasi intelijen bisnis, dan aplikasi grafis.

PowerPro bundel

Bundel ini sangat cocok untuk yang berikut:

- Penjelajahan web
- Pengolah kata
- Email
- Pesan instan
- Spreadsheet
- Pemrosesan audio
- Pengembangan perangkat lunak (Integrated Development Environment (IDE))
- Pergudangan data
- Aplikasi intelijen bisnis
- Konferensi audio dan video

Bundel ini tidak direkomendasikan untuk pelatihan model pembelajaran mesin, dan aplikasi grafis

GraphicsPro bundel

Bundel ini menawarkan tingkat kinerja grafis dasar, dan kinerja CPU dan memori tingkat tinggi untuk Anda. WorkSpaces Sangat cocok untuk yang berikut:

- Penjelajahan web
- Pengolah kata
- Email
- Pesan instan
- Spreadsheet
- Konferensi audio
- Pengembangan perangkat lunak (Integrated Development Environment (IDE))
- Pergudangan data
- Aplikasi intelijen bisnis
- Desain grafis
- Pemrosesan gambar

Bundel ini tidak direkomendasikan untuk konferensi audio dan video, rendering 3D, dan desain foto-realistis

Graphics.g4dn bundel

Bundel ini menawarkan kinerja grafis tingkat tinggi, dan tingkat kinerja CPU dan memori moderat untuk Anda WorkSpaces dan sangat cocok untuk hal-hal berikut:

- Penjelajahan web
- Pengolah kata
- Email
- Spreadsheet
- Pesan instan
- Konferensi audio
- Pengembangan perangkat lunak (Integrated Development Environment (IDE))
- Masuk ke pemrosesan data tingkat menengah
- Pergudangan data
- Aplikasi intelijen bisnis
- Desain grafis
- CAD/CAM (desain berbantuan komputer/manufaktur berbantuan komputer)

Bundel ini tidak direkomendasikan untuk konferensi audio dan video, rendering 3D, desain foto-realistis, dan pelatihan model pembelajaran mesin

GraphicsPro.g4dn

GraphicsPro.g4dn bundel

Bundel ini menawarkan kinerja grafis, kinerja CPU, dan memori tingkat tinggi untuk Anda WorkSpaces dan sangat cocok untuk hal-hal berikut:

- Penjelajahan web
- Pengolah kata
- Email
- Spreadsheet
- Pesan instan

- Konferensi audio
- Pengembangan perangkat lunak (Integrated Development Environment (IDE))
- Masuk ke pemrosesan data tingkat menengah
- Pergudangan data
- Aplikasi intelijen bisnis
- Desain grafis
- CAD/CAM (desain berbantuan komputer/manufaktur berbantuan komputer)
- Transcoding video
- Rendering 3D
- Desain foto-realistis
- Streaming permainan
- Pelatihan model ML (machine learning) dan inferensi ML

Bundel ini tidak disarankan untuk konferensi audio dan video.

Buat WorkSpaces gambar dan bundel khusus

Jika Anda telah meluncurkan Windows atau Linux WorkSpace dan telah menyesuaikannya, Anda dapat membuat gambar khusus dan bundel khusus dari itu WorkSpace.

Gambar khusus hanya berisi OS, perangkat lunak, dan pengaturan untuk WorkSpace. Bundel kustom adalah kombinasi dari gambar kustom dan perangkat keras dari mana a WorkSpace dapat diluncurkan.

> **Note**
>
> Pastikan Anda menunggu setidaknya 2 jam setelah menghapus bundel sebelum membuat bundel baru dengan nama yang sama.

Setelah Anda membuat citra kustom, Anda dapat membangun paket kustom yang menggabungkan citra kustom dan konfigurasi dasar komputasi dan penyimpanan yang Anda pilih. Anda kemudian dapat menentukan bundel kustom ini ketika Anda meluncurkan baru WorkSpaces untuk memastikan

bahwa yang baru WorkSpaces memiliki konfigurasi konsisten yang sama (perangkat keras dan perangkat lunak).

Anda dapat menggunakan citra kustom yang sama untuk membuat berbagai paket kustom dengan memilih opsi komputasi dan penyimpanan berbeda untuk setiap paket.

Important

- Jika Anda berencana untuk membuat gambar dari Windows 10 WorkSpace, perhatikan bahwa pembuatan gambar tidak didukung pada sistem Windows 10 yang telah ditingkatkan dari satu versi Windows 10 ke versi Windows 10 yang lebih baru (peningkatan fitur/versi Windows). Namun, pembaruan kumulatif atau keamanan Windows didukung oleh proses pembuatan WorkSpaces gambar.
- Setelah 14 Januari 2020, citra tidak dapat dibuat dari paket Windows 7 publik. Anda mungkin ingin mempertimbangkan untuk memigrasi Windows 7 Anda WorkSpaces ke Windows 10. Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.
- Bundel grafis tidak lagi didukung setelah 30 November 2023. Kami merekomendasikan untuk memigrasikan paket Anda WorkSpaces ke Graphics.g4dn. Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.
- Grafik dan GraphicsPro bundel saat ini tidak tersedia di Wilayah Asia Pasifik (Mumbai).
- Volume penyimpanan bundel khusus tidak boleh lebih kecil dari volume penyimpanan gambar.

Paket kustom memiliki biaya yang sama dengan paket publik tempat paket dibuat. Untuk informasi selengkapnya tentang harga, lihat WorkSpaces Harga Amazon.

Daftar Isi

- Apa yang disertakan dengan gambar WorkSpace kustom Linux

Persyaratan membuat citra kustom Windows

> **Note**
>
> Windows saat ini mendefinisikan 1 GB sebagai 1.073.741.824 byte. Pelanggan perlu memastikan bahwa mereka memiliki lebih dari 12.884.901.888 byte (atau 12 GiB) gratis pada drive C dan profil pengguna kurang dari 10.737.418.240 byte (atau 10 GiB) untuk membuat gambar a. WorkSpace

- Status WorkSpace harus Tersedia dan status modifikasinya harus Tidak Ada.
- Semua aplikasi dan profil pengguna pada WorkSpaces gambar harus kompatibel dengan Microsoft Sysprep.
- Semua aplikasi untuk disertakan dalam gambar harus diinstal pada `C` drive.
- Untuk Windows 7 WorkSpaces, dan ukuran totalnya (file dan data) harus kurang dari 10 GB.
- Untuk Windows 7 WorkSpaces, `C` drive harus memiliki setidaknya 12 GB ruang yang tersedia.
- Semua layanan aplikasi yang berjalan di WorkSpace harus menggunakan akun sistem lokal alih-alih kredensi pengguna domain. Misalnya, Anda tidak dapat memiliki instalasi Microsoft SQL Server Express yang berjalan dengan kredensial pengguna domain.
- Tidak WorkSpace boleh dienkripsi. Pembuatan gambar dari terenkripsi saat WorkSpace ini tidak didukung.
- Komponen berikut diperlukan dalam citra. Tanpa komponen ini, WorkSpaces yang Anda luncurkan dari gambar tidak akan berfungsi dengan benar. Untuk informasi selengkapnya, lihat the section called “Konfigurasi yang diperlukan”.
  - Windows PowerShell versi 3.0 atau yang lebih baru
  - Layanan Desktop Jarak Jauh
  - AWS Driver PV
  - Manajemen Jarak Jauh Windows (WinRM)
  - Agen dan driver Teradici PCoIP
  - Agen dan driver STXHD
  - AWS dan WorkSpaces sertifikat

- Agen Skylight

Persyaratan untuk membuat gambar kustom Linux

- Status WorkSpace harus Tersedia dan status modifikasinya harus Tidak Ada.
- Semua aplikasi untuk disertakan dalam gambar harus diinstal di luar volume pengguna (`/home`direktori).
- Volume akar (/) harus kurang dari 97% penuh.
- Tidak WorkSpace boleh dienkripsi. Pembuatan gambar dari terenkripsi saat WorkSpace ini tidak didukung.
- Komponen berikut diperlukan dalam citra. Tanpa komponen ini, WorkSpaces yang Anda luncurkan dari gambar tidak akan berfungsi dengan benar:
  - Cloud-init
  - Teradici PCoIP atau agen dan driver WSP
  - Agen Skylight

Praktik terbaik

Sebelum Anda membuat gambar dari a WorkSpace, lakukan hal berikut:

- Gunakan VPC terpisah yang tidak terhubung ke lingkungan produksi Anda.
- Terapkan WorkSpace di subnet pribadi dan gunakan instance NAT untuk lalu lintas keluar.
- Gunakan direktori Simple AD kecil.
- Gunakan ukuran volume terkecil untuk sumber WorkSpace, dan kemudian sesuaikan ukuran volume sesuai kebutuhan saat membuat bundel khusus.
- Instal semua pembaruan sistem operasi (kecuali pembaruan fitur/versi Windows) dan semua pembaruan aplikasi di file. WorkSpace Untuk informasi lebih lanjut, lihat bagian Catatan penting di awal topik ini.
- Hapus data cache dari WorkSpace yang seharusnya tidak disertakan dalam bundel (misalnya, riwayat browser, file cache, dan cookie browser).
- Hapus pengaturan konfigurasi dari WorkSpace yang seharusnya tidak disertakan dalam bundel (misalnya, profil email).
- Beralih ke pengaturan alamat IP dinamik menggunakan DHCP.

- Pastikan Anda belum melebihi kuota untuk WorkSpace gambar yang diizinkan di Wilayah. Secara default, Anda diizinkan 40 WorkSpace gambar per Wilayah. Jika Anda telah mencapai kuota ini, upaya baru untuk membuat citra akan gagal. Untuk meminta kenaikan kuota, gunakan formulir WorkSpaces Limits.
- Pastikan Anda tidak mencoba membuat gambar dari yang dienkripsi WorkSpace. Pembuatan gambar dari terenkripsi saat WorkSpace ini tidak didukung.
- Jika Anda menjalankan perangkat lunak antivirus apa pun WorkSpace, nonaktifkan saat Anda mencoba membuat gambar.
- Jika Anda mengaktifkan firewall WorkSpace, pastikan firewall tidak memblokir port yang diperlukan. Untuk informasi selengkapnya, lihat Alamat IP dan persyaratan port untuk WorkSpaces.
- Untuk Windows WorkSpaces, jangan mengonfigurasi Objek Kebijakan Grup (GPO) apa pun sebelum pembuatan gambar.
- Untuk Windows WorkSpaces, jangan menyesuaikan profil pengguna default (`C:\Users \Default`) sebelum membuat gambar. Kami merekomendasikan membuat penyesuaian apa pun ke profil pengguna melalui GPO, dan menerapkannya setelah pembuatan citra. GPO dapat dengan mudah diubah atau digulung kembali, dan karena itu lebih tahan terhadap kesalahan daripada kustomisasi yang dibuat untuk profil pengguna default.
- Untuk Linux WorkSpaces, lihat juga whitepaper “Praktik Terbaik untuk Mempersiapkan Amazon Anda WorkSpaces untuk Gambar Linux”.
- Jika Anda ingin menggunakan kartu pintar di Linux WorkSpaces dengan WorkSpaces Streaming Protocol (WSP) diaktifkan, lihat Gunakan kartu pintar untuk autentikasi penyesuaian yang harus Anda buat untuk Linux Anda WorkSpace sebelum membuat gambar Anda.
- Pastikan Anda memperbarui driver ketergantungan jaringan seperti driver ENA, NVMe, dan PV pada Anda. WorkSpaces Anda harus melakukan ini setidaknya sekali setiap 6 bulan. Untuk informasi selengkapnya, lihat Menginstal atau memutakhirkan driver Elastic Network Adapter (ENA), Driver AWS NVMe untuk instance Windows, dan Upgrade driver PV pada instans Windows.
- Pastikan Anda memperbarui agen EC2config, EC2launch, dan EC2launch V2 ke versi terbaru secara berkala. Anda harus melakukan ini setidaknya sekali setiap 6 bulan. Untuk informasi selengkapnya, lihat Memperbarui EC2config dan EC2launch.

(Opsional) Langkah 1: Menentukan format nama komputer kustom untuk citra Anda

Untuk yang WorkSpaces diluncurkan dari gambar kustom atau Bring Your Own License (BYOL), Anda dapat menentukan awalan khusus untuk format nama komputer alih-alih menggunakan format nama komputer default. Untuk menentukan prefiks kustom, ikuti prosedur yang sesuai untuk tipe citra Anda.

Untuk menentukan format nama komputer kustom untuk citra kustom

1. Pada WorkSpace yang Anda gunakan untuk membuat gambar kustom Anda, buka `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` di Notepad atau editor teks lain. Untuk informasi lebih lanjut tentang bekerja dengan file `Unattend.xml`, lihat File jawaban (unattend.xml) dalam dokumentasi Microsoft.

   > **Note**
   >
   > Untuk mengakses drive C: dari Windows File Explorer pada Anda WorkSpace, masukkan **`C:\`** di bilah alamat.

2. Di bagian `<settings pass="specialize">`, pastikan bahwa `<ComputerName>` diatur ke tanda bintang (`*`). Jika `<ComputerName>` diatur ke nilai lain, pengaturan nama komputer kustom Anda akan diabaikan. Untuk informasi selengkapnya tentang `<ComputerName>` pengaturan, lihat ComputerNamedi dokumentasi Microsoft.
3. Di bagian `<settings pass="specialize">`, tetapkan `<RegisteredOrganization>` dan `<RegisteredOwner>` ke nilai pilihan Anda.

   Selama Sysprep, nilai yang Anda tentukan untuk `<RegisteredOwner>` dan`<RegisteredOrganization>` digabungkan, dan 7 karakter pertama dari string gabungan digunakan untuk membuat nama komputer. *Misalnya, jika Anda menentukan* ***Amazon.com*** *untuk <RegisteredOrganization> dan untuk<RegisteredOwner>, nama komputer* ***EC2*** *untuk yang WorkSpaces dibuat dari bundel kustom Anda akan dimulai dengan EC2AMAZ- xxxxxxx.*

> **Note**
>
> Nilai <RegisteredOrganization> dan <RegisteredOwner> nilai dalam bagian <settings pass="oobeSystem"> diabaikan oleh Sysprep.

4. Simpan perubahan Anda ke file Unattend.xml.

Untuk menentukan format nama komputer kustom untuk citra kustom

1. Jika Anda menggunakan Windows 10, buka C:\Program Files\Amazon \Ec2ConfigService\Sysprep2008.xml di Notepad atau editor teks lain. Jika Anda menggunakan Windows 11, bukaC:\ProgramData\Amazon\EC2Launch\sysprep \OOBE_unattend.xml.
2. Di bagian <settings pass="specialize">, batalkan komentar <ComputerName>*</ ComputerName>, dan pastikan <ComputerName> diatur ke tanda bintang (*). Jika <ComputerName> diatur ke nilai lain, pengaturan nama komputer kustom Anda akan diabaikan. Untuk informasi selengkapnya tentang <ComputerName> pengaturan, lihat ComputerNamedi dokumentasi Microsoft.
3. Di bagian <settings pass="specialize">, tetapkan <RegisteredOrganization> dan <RegisteredOwner> ke nilai pilihan Anda.

   Selama Sysprep, nilai yang Anda tentukan untuk <RegisteredOwner> dan<RegisteredOrganization> digabungkan, dan 7 karakter pertama dari string gabungan digunakan untuk membuat nama komputer. *Misalnya, jika Anda menentukan* ***Amazon.com*** *untuk <RegisteredOrganization> dan untuk<RegisteredOwner>, nama komputer* ***EC2*** *untuk yang WorkSpaces dibuat dari bundel kustom Anda akan dimulai dengan EC2AMAZ- xxxxxxx.*

   > **Note**
   >
   > Nilai <RegisteredOrganization> dan <RegisteredOwner> nilai dalam bagian <settings pass="oobeSystem"> diabaikan oleh Sysprep.

4. Jika Anda menggunakan Windows 10, simpan perubahan Anda ke Sysprep2008.xml file. Jika Anda menggunakan Windows 11, simpan perubahan Anda ke OOBE_unattend.xml

Langkah 2: Jalankan Pemeriksa Citra

> **Note**
>
> Pemeriksa Gambar hanya tersedia untuk Windows WorkSpaces. Jika Anda membuat gambar dari Linux WorkSpace, lewati keLangkah 3: Buat citra dan paket kustom.

Untuk mengonfirmasi bahwa Windows Anda WorkSpace memenuhi persyaratan untuk pembuatan gambar, sebaiknya jalankan Pemeriksa Gambar. Pemeriksa Gambar melakukan serangkaian pengujian WorkSpace yang ingin Anda gunakan untuk membuat gambar Anda, dan memberikan panduan tentang cara mengatasi masalah apa pun yang ditemukannya.

> **Important**
>
> - WorkSpace Harus lulus semua tes yang dijalankan oleh Pemeriksa Gambar sebelum Anda dapat menggunakannya untuk pembuatan gambar.
> - Sebelum Anda menjalankan Pemeriksa Gambar, verifikasi bahwa keamanan Windows terbaru dan pembaruan kumulatif diinstal pada Anda. WorkSpace

Untuk mendapatkan Pemeriksa Citra, lakukan salah satu hal berikut:

- Reboot Anda WorkSpace. Pemeriksa Citra diunduh secara otomatis selama booting ulang dan diinstal di `C:\Program Files\Amazon\ImageChecker.exe`.
- Unduh Pemeriksa WorkSpaces Gambar Amazon dari https://tools.amazonworkspaces.com/ImageChecker .zip dan ekstrak file. `ImageChecker.exe` Salin file ke `C:\Program Files\Amazon\`.

Untuk Menjalankan Pemeriksa Citra

1. Buka file `C:\Program Files\Amazon\ImageChecker.exe`.
2. Di kotak dialog Amazon WorkSpaces Image Checker, pilih Jalankan.
3. Setelah menyelesaikan setiap tes, Anda dapat melihat status tes.

Untuk setiap tes dengan status GAGAL, pilih Info untuk menampilkan informasi penyelesaian masalah yang menyebabkan kegagalan. Untuk informasi penyelesaian masalah ini, lihat Tips untuk menyelesaikan masalah yang terdeteksi oleh Pemeriksa Citra.

Jika ada pengujian yang menampilkan status PERINGATAN, pilih tombol Perbaiki Semua Peringatan.

Alat ini menghasilkan berkas log output dalam direktori yang sama tempat Pemeriksa Citra berada. Secara default, file ini terletak di `C:\Program Files\Amazon \ImageChecker_yyyyMMddhhmmss.log`.

> **Tip**
>
> Jangan hapus berkas log ini. Jika terjadi masalah, berkas log ini dapat membantu dalam pemecahan masalah.

4. Jika berlaku, selesaikan masalah apa pun yang menyebabkan kegagalan pengujian dan peringatan, dan ulangi proses menjalankan Pemeriksa Gambar hingga WorkSpace lulus semua pengujian. Semua kegagalan dan peringatan harus diselesaikan sebelum Anda dapat membuat citra.
5. Setelah WorkSpace melewati semua tes, Anda akan melihat pesan Validasi Berhasil. Kini Anda siap membuat paket kustom.

Tips untuk menyelesaikan masalah yang terdeteksi oleh Pemeriksa Citra

Selain berkonsultasi tips penyelesaian masalah berikut yang terdeteksi oleh Pemeriksa Citra, pastikan meninjau berkas log Pemeriksa Citra di `C:\Program Files\Amazon \ImageChecker_yyyyMMddhhmmss.log`.

PowerShell versi 3.0 atau yang lebih baru harus diinstal

Instal versi terbaru Microsoft Windows PowerShell.

> **Important**
>
> Kebijakan PowerShell eksekusi untuk a WorkSpace harus disetel untuk mengizinkan RemoteSignedskrip. Untuk memeriksa kebijakan eksekusi, jalankan ExecutionPolicy PowerShell perintah Get-. Jika kebijakan eksekusi tidak disetel ke Tidak Dibatasi atau

RemoteSigned, jalankan ExecutionPolicy RemoteSigned perintah Set- ExecutionPolicy — untuk mengubah nilai kebijakan eksekusi. RemoteSignedPengaturan memungkinkan eksekusi skrip di Amazon WorkSpaces, yang diperlukan untuk membuat gambar.

Hanya drive C dan D yang dapat hadir

Hanya `D` drive `C` dan yang dapat hadir pada WorkSpace yang digunakan untuk pencitraan. Hapus semua drive lainnya, termasuk drive virtual.

Tidak ada booting ulang tertunda karena Pembaruan Windows dapat dideteksi

- Proses Create Image tidak dapat berjalan sampai Windows di-boot ulang untuk menyelesaikan instalasi keamanan atau pembaruan kumulatif. Booting ulang Windows untuk menerapkan pembaruan ini, dan pastikan bahwa tidak ada pembaruan keamanan atau kumulatif Windows lainnya yang perlu diinstal tertunda.
- Pembuatan citra tidak didukung pada sistem Windows 10 yang telah ditingkatkan dari satu versi Windows 10 ke versi Windows 10 yang lebih baru (peningkatan fitur/versi Windows). Namun, pembaruan kumulatif atau keamanan Windows didukung oleh proses pembuatan WorkSpaces gambar.

File Sysprep harus ada dan tidak boleh kosong

Jika terdapat masalah dengan file Sysprep Anda, hubungiPusat AWS Support agar EC2config atau EC2Launch Anda diperbaiki.

Ukuran profil pengguna harus kurang dari 10 GB

Untuk Windows 7 WorkSpaces, profil pengguna (`D:\Users\`*`username`*) harus kurang dari 10 GB total. Hapus file sesuai keperluan untuk mengurangi ukuran profil pengguna.

Drive C harus memiliki ruang kosong yang cukup

Untuk Windows 7 WorkSpaces, Anda harus memiliki setidaknya 12 GB ruang kosong pada driveC. Hapus file sesuai kebutuhan untuk mengosongkan ruang pada drive `C`. Untuk Windows 10 WorkSpaces, abaikan jika Anda menerima `FAILED` pesan dan ruang disk di atas 2GB.

Tidak ada layanan yang dapat berjalan di akun domain

Untuk menjalankan proses Create Image, tidak ada layanan yang WorkSpace dapat berjalan di bawah akun domain. Semua layanan harus berjalan di akun lokal.

Untuk menjalankan layanan di bawah akun lokal

1. Buka `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` dan temukan daftar layanan yang berjalan di bawah akun domain.
2. Di kotak pencarian Windows, masukkan **`services.msc`** untuk membuka Windows Services Manager.
3. Di Log On Sebagai, cari layanan yang berjalan di akun domain. (Layanan yang berjalan sebagai Sistem Lokal, Layanan Lokal, atau Layanan Jaringan tidak mengganggu pembuatan citra.)
4. Pilih layanan yang berjalan di akun domain, dan lalu pilihTindakan, Properti.
5. Buka tab Log On. Di Log on sebagai, pilih Akun Sistem Lokal.
6. Pilih OKE.

WorkSpace Harus dikonfigurasi untuk menggunakan DHCP

Anda harus mengkonfigurasi semua adapter jaringan pada WorkSpace untuk menggunakan DHCP bukan alamat IP statis.

Untuk mengatur semua adapter jaringan agar menggunakan DHCP

1. Di kotak pencarian Windows, masukkan **`control panel`** untuk membuka Panel Kontrol.
2. Pilih Jaringan dan Internet.
3. Pilih Jaringan dan Pusat Berbagi.
4. Pilih Mengubah pengaturan adapter, dan pilih adapter.
5. Pilih Ubah pengaturan hubungan ini.
6. Pada tab Jaringan, pilih Internet Protocol Version 4 (TCP/IPv4), lalu pilih Properti.
7. Di kotak dialog Properti Internet Protocol Version 4 (TCP/IPv4), pilih Dapatkan alamat IP secara otomatis.
8. Pilih OKE.
9. Ulangi proses ini untuk semua adapter jaringan di file WorkSpace.

Layanan Desktop Jarak Jauh harus diaktifkan

Proses Pembuatan Citra perlu Layanan Desktop Jarak Jauh yang aktif.

Untuk mengaktifkan Layanan Desktop Jarak Jauh

1. Di kotak pencarian Windows, masukkan **`services.msc`** untuk membuka Windows Services Manager.
2. Di kolom Nama, cari Layanan Desktop Jarak Jauh.
3. Pilih Layanan Desktop Jarak Jauh, lalu pilihTindakan, Properti.
4. Pada tab Umum, untuk Tipe Startup, pilih Manual atau Otomatis.
5. Pilih OKE.

Profil pengguna harus ada

WorkSpace Yang Anda gunakan untuk membuat gambar harus memiliki profil pengguna (`D:\Users\`*`username`*). Jika pengujian ini gagal, hubungi Pusat AWS Support untuk mendapatkan bantuan.

Jalur variabel lingkungan harus dikonfigurasi dengan benar

Jalur variabel lingkungan untuk mesin lokal tidak memiliki entri untuk System32 dan untuk Windows. PowerShell Entri ini diperlukan agar pembuatan citra berjalan.

Untuk mengonfigurasi jalur variabel lingkungan

1. Di kotak pencarian Windows, masukkan **`environment variables`** lalu pilih Edit variabel lingkungan sistem.
2. Dalam kotak dialog Properti Sistem, pilih tab Lanjutan, dan pilih Variabel Lingkungan.
3. Di kotak dialog Variabel lingkungan, di Variabel sistem, pilih Jalur lalu pilih Edit.
4. Pilih Baru, dan tambahkan jalur berikut:

   ```
   C:\Windows\System32
   ```
5. Pilih Baru kembali, dan tambahkan jalur berikut:

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```
6. Pilih OKE.
7. Mulai ulang WorkSpace.

> **Tip**
>
> Urutan item yang muncul di jalur lingkungan variabel adalah hal penting. Untuk menentukan urutan yang benar, Anda mungkin ingin membandingkan jalur variabel

lingkungan Anda WorkSpace dengan jalur dari instance Windows yang baru dibuat WorkSpace atau yang baru.

Penginstal Modul Windows harus diaktifkan

Proses Pembuatan Citra perlu layanan Penginstal Modul Windows yang aktif.

Untuk mengaktifkan layanan Penginstal Modul Windows

1. Di kotak pencarian Windows, masukkan **`services.msc`** untuk membuka Windows Services Manager.
2. Di kolom Nama, cari Penginstal Modul Windows.
3. Pilih Penginstal Modul Windows, lalu pilih Tindakan, Properti.
4. Pada tab Umum, untuk Tipe Startup, pilih Manual atau Otomatis.
5. Pilih OKE.

Amazon SSM Agent harus dinonaktifkan

Proses pembuatan citra memerlukan layanan Amazon SSM Agent dinonaktifkan.

Untuk menonaktifkan layanan Amazon SSM Agent

1. Di kotak pencarian Windows, masukkan **`services.msc`** untuk membuka Windows Services Manager.
2. Di kolom Nama, cari Amazon SSM Agent.
3. Pilih Amazon SSM Agent, lalu pilih Tindakan, Properti.
4. Pada tab Umum, untuk Tipe Startup, PilihNonaktif.
5. Pilih OKE.

SSL3 dan TLS versi 1.2 harus diaktifkan

Untuk mengonfigurasi SSL/TLS untuk Windows, lihat Cara mengaktifkan TLS 1.2 dalam dokumentasi Microsoft Windows.

Hanya satu profil pengguna yang dapat ada di WorkSpace

Hanya ada satu profil WorkSpaces pengguna (`D:\Users\`*`username`*) pada WorkSpace yang Anda gunakan untuk membuat gambar. Hapus profil pengguna yang bukan milik pengguna yang dituju WorkSpace.

Agar pembuatan gambar berfungsi, Anda hanya WorkSpace dapat memiliki tiga profil pengguna di dalamnya:

- Profil pengguna pengguna yang dituju dari WorkSpace (`D:\Users\`*`username`*)
- Profil pengguna default (juga dikenal sebagai Default Profile)
- Profil pengguna Administrator

Jika ada profil pengguna tambahan, Anda dapat menghapusnya melalui properti sistem lanjutan di Panel Kontrol Windows.

Untuk menghapus profil pengguna

1. Untuk mengakses properti sistem lanjutan, lakukan salah satu hal berikut:
   - Tekan Kunci Windows+Jeda Istirahat, lalu pilih Pengaturan sistem lanjutan dalam panel kiri dari Panel Kontrol > Sistem dan Keamanan > kotak dialog Sistem.
   - Dalam kotak pencarian Windows, masukkan **`control panel`**. Di Panel Kontrol, pilih Sistem dan Keamanan, lalu pilih Sistem, pilih Pengaturan sistem lanjutan dalam panel kiri di Panel Kontrol > Sistem dan Keamanan > kotak dialog Sistem.
2. Di kotak dialog Properti Sistem, pada tab Lanjutan, pilih Pengaturan di Profil Pengguna.
3. Jika ada profil yang terdaftar selain profil Administrator, Profil Default, dan profil WorkSpaces pengguna yang dituju, pilih profil tambahan itu dan pilih Hapus.
4. Saat ditanya keinginan menghapus profil, pilih Ya.
5. Jika perlu, ulangi Langkah 3 dan 4 untuk menghapus profil lain yang tidak termasuk dalam WorkSpace.
6. Pilih OKE dua kali dan tutup Panel Kontrol.
7. Mulai ulang WorkSpace.

Paket AppX tidak bisa berada dalam keadaan bertahap

Satu paket AppX atau lebih berada dalam keadaan bertahap. Hal ini dapat menyebabkan kesalahan Sysprep selama pembuatan citra.

Untuk menghapus semua paket AppX yang dipaketkan

1. Dalam kotak pencarian Windows, masukkan **`powershell`**. Pilih Jalankan sebagai Administrator.
2. Saat ditanya "Apakah Anda ingin mengizinkan aplikasi ini melakukan perubahan pada perangkat?", PilihYa.
3. Di PowerShell jendela Windows, masukkan perintah berikut untuk mencantumkan semua paket AppX bertahap, dan tekan Enter setelah masing-masing.

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                ($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                (!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                $_.PackageUserInformation -like "*Staged*")
                                }
```

4. Masukkan perintah berikut untuk menghapus semua paket AppX bertahap, lalu tekan Enter.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Untuk Menjalankan Pemeriksa Citra Jika ujian ini masih gagal, masukkan perintah berikut untuk menghapus semua paket AppX, dan tekan Enter setelah setiap paket.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows tidak harus telah ditingkatkan dari versi sebelumnya

Pembuatan citra tidak didukung pada sistem Windows yang telah ditingkatkan dari satu versi Windows 10 ke versi Windows 10 yang lebih baru (peningkatan fitur/versi Windows).

Untuk membuat gambar, gunakan WorkSpace yang belum mengalami peningkatan fitur/versi Windows.

Jumlah Windows persenjataan ulang tidak boleh 0

Fitur persenjataan ulang memungkinkan Anda memperpanjang masa aktivasi untuk versi percobaan Windows. Proses Pembuatan Citra mengharuskan jumlah persenjataan ulang bernilai selain 0.

Untuk memeriksa jumlah persenjataan ulang Windows

1. Pada menu Mulai Windows, pilihSistem Windows, lalu pilih Perintah.
2. Dalam jendela Perintah, masukkan perintah berikut, kemudian tekan Enter.

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

Untuk mengatur ulang jumlah persenjataan ulang ke nilai selain 0, lihat Instalasi Windows Sysprep (Generalize) dalam dokumentasi Microsoft Windows.

Tips penyelesaian masalah lainnya

Jika Anda WorkSpace lulus semua pengujian yang dijalankan oleh Pemeriksa Gambar, tetapi Anda masih tidak dapat membuat gambar dari WorkSpace, periksa masalah berikut:

- Pastikan WorkSpace tidak ditetapkan ke pengguna dalam grup Tamu Domain. Untuk memeriksa apakah ada akun domain, jalankan PowerShell perintah berikut.

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
$env:USERDOMAIN*" }
```

- Untuk Windows 7 WorkSpaces saja: Jika masalah terjadi saat profil pengguna sedang disalin selama pembuatan gambar, periksa masalah berikut:
  - Jalur profil panjang dapat menyebabkan kesalahan pembuatan citra. Pastikan bahwa jalur semua folder dalam profil pengguna kurang dari 261 karakter.
  - Pastikan untuk memberikan izin penuh pada folder profil untuk sistem dan semua paket aplikasi.

  - Jika file dalam profil pengguna terkunci oleh proses atau sedang digunakan selama pembuatan citra, penyalinan profil berpotensi gagal.
- Beberapa Group Policy Objects (GPO) membatasi akses ke sidik jari sertifikat RDP ketika diminta oleh layanan EC2Config atau skrip EC2Launch selama konfigurasi instans Windows. Sebelum Anda mencoba membuat gambar, pindahkan WorkSpace ke unit organisasi baru (OU) dengan warisan yang diblokir dan tidak ada GPO yang diterapkan.
- Pastikan bahwa layanan Windows Remote Management (WinRM) dikonfigurasi untuk memulai secara otomatis. Lakukan hal-hal berikut:
  1. Di kotak pencarian Windows, masukkan **`services.msc`** untuk membuka Windows Services Manager.
  2. Di kolom Nama, cari Manajemen Jarak Jauh Windows (WS-Management).
  3. Pilih Manajemen Jarak Jauh Windows (WS-Management), lalu pilih Tindakan, Properti.
  4. Pada tab Umum, untuk Tipe Startup, pilih Otomatis.
  5. Pilih OKE.

Langkah 3: Buat citra dan paket kustom

Setelah Anda memvalidasi WorkSpace gambar Anda, Anda dapat melanjutkan dengan membuat gambar kustom dan bundel kustom Anda.

Buat citra dan paket kustom

1. Jika Anda masih terhubung ke WorkSpace, putuskan sambungan dengan memilih Amazon WorkSpaces dan Putuskan sambungan di aplikasi WorkSpaces klien.
2. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
3. Di panel navigasi, pilih WorkSpaces.
4. Pilih WorkSpace untuk membuka halaman detailnya dan pilih Buat gambar. Jika status WorkSpace Dihentikan, Anda harus memulainya terlebih dahulu (pilih Tindakan, Mulai WorkSpaces) sebelum Anda dapat memilih Tindakan, Buat Gambar.

> **Note**
>
> Untuk membuat gambar secara terprogram, gunakan tindakan CreateWorkspaceImage API. Untuk informasi selengkapnya, lihat CreateWorkspaceImagedi Referensi Amazon WorkSpaces API.

5. Sebuah pesan ditampilkan, meminta Anda untuk reboot (restart) Anda WorkSpace sebelum melanjutkan. Mem-boot ulang WorkSpace pembaruan WorkSpaces perangkat lunak Amazon Anda ke versi terbaru.

   Reboot Anda WorkSpace dengan menutup pesan dan mengikuti langkah-langkahnyaNyalakan ulang WorkSpace. Setelah selesai, ulangi Step 4 prosedur ini, tetapi kali ini pilih Selanjutnya saat pesan boot ulang muncul. Untuk membuat gambar, status WorkSpace harus Tersedia dan status modifikasinya harus Tidak Ada.

6. Masukkan nama citra dan deskripsi yang akan membantu Anda mengidentifikasi citra, lalu pilih Buat Citra. Saat gambar sedang dibuat, status WorkSpace ditangguhkan dan tidak WorkSpace tersedia.

7. Di panel navigasi, pilih Citra. Gambar selesai ketika status WorkSpace perubahan ke Tersedia (ini bisa memakan waktu hingga 45 menit).

8. Pilih citra dan pilih Tindakan, Buat Paket.

> **Note**
>
> Untuk membuat paket secara terprogram, gunakan Tindakan API CreateWorkspaceBundle. Untuk informasi selengkapnya, lihat CreateWorkspaceBundledi Referensi Amazon WorkSpaces API.

9. Masukkan nama paket dan deskripsi, lalu lakukan hal berikut:

   - Untuk jenis perangkat keras Bundel, pilih perangkat keras yang akan digunakan saat meluncurkan WorkSpaces dari bundel khusus ini.
   - Untuk Pengaturan penyimpanan, pilih salah satu kombinasi default untuk volume akar dan ukuran volume pengguna, atau pilih Kustom, lalu masukkan nilai (hingga 2000 GB) untuk Ukuran volume akar dan Ukuran volume pengguna.

Kombinasi ukuran default yang tersedia untuk volume akar (untuk Microsoft Windows, drive `C`, untuk Linux,/) dan volume pengguna (untuk Windows, drive `D`; untuk Linux, /home) adalah sebagai berikut:

- Akar: 80 GB, Pengguna: 10 GB, 50 GB, atau 100 GB
- Akar: 175 GB, Pengguna: 100 GB
- Untuk Graphics.g4dn, GraphicsPro .g4dn, Grafik, dan GraphicsPro WorkSpaces hanya: Root: 100 GB, Pengguna: 100 GB

Atau, Anda dapat memperluas akar dan volume pengguna hingga 2000 GB masing-masing.

> **Note**
>
> Untuk memastikan bahwa data Anda dipertahankan, Anda tidak dapat mengurangi ukuran root atau volume pengguna setelah Anda meluncurkan file WorkSpace. Sebagai gantinya, pastikan Anda menentukan ukuran minimum untuk volume ini saat meluncurkan file WorkSpace. Anda dapat meluncurkan Nilai, Standar, Kinerja, Daya, atau PowerPro WorkSpace dengan minimal 80 GB untuk volume root dan 10 GB untuk volume pengguna. Anda dapat meluncurkan Graphics.g4dn, GraphicsPro .g4dn, Graphics, atau GraphicsPro WorkSpace dengan minimal 100 GB untuk volume root dan 100 GB untuk volume pengguna.

10. Pilih Buat paket.
11. Untuk mengonfirmasi bahwa paket Anda telah dibuat, pilih Paket dan verifikasi bahwa paket terdaftar.

Apa yang disertakan dengan gambar WorkSpaces kustom Windows

Saat Anda membuat gambar dari Windows 7, Windows 10, atau Windows 11 WorkSpace, seluruh konten `C` drive disertakan.

Untuk Windows 10 atau 11 WorkSpaces, profil pengguna di `D:\Users\`*`username`* tidak termasuk dalam gambar khusus.

Untuk Windows 7 WorkSpaces, seluruh konten profil pengguna `D:\Users\`*`username`* disertakan, kecuali untuk yang berikut ini:

- Kontak

- Unduh
- Musik
- Gambar
- Game yang disimpan
- Video
- Podcast
- mesin virtual
- .virtualbox
- Pelacakan
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\

- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Apa yang disertakan dengan gambar WorkSpace kustom Linux

Saat Anda membuat gambar dari Amazon Linux WorkSpace, seluruh isi volume pengguna (/home) akan dihapus. Isi volume root (/) disertakan, kecuali folder dan kunci berikut yang berlaku, yang dihapus:

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/ zz-workspaces-domain .yaml
- /etc/netplan/ yy-workspaces-base .yaml

- /var/lib/ /pengguna AccountsService

Tombol berikut terpecah selama pembuatan citra kustom:

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

Perbarui WorkSpaces bundel khusus

Anda dapat memperbarui WorkSpaces bundel kustom yang ada dengan memodifikasi WorkSpace yang didasarkan pada bundel, membuat gambar dari WorkSpace, dan memperbarui bundel dengan gambar baru. Anda kemudian dapat meluncurkan baru WorkSpaces menggunakan bundel yang diperbarui.

> **Important**
>
> Yang ada WorkSpaces tidak diperbarui secara otomatis saat Anda memperbarui bundel yang menjadi dasarnya. Untuk memperbarui WorkSpaces yang ada yang didasarkan pada bundel yang telah Anda perbarui, Anda harus membangun kembali WorkSpaces atau menghapus dan membuatnya kembali.

Untuk memperbarui paket menggunakan konsol tersebut

1. Connect ke WorkSpace yang didasarkan pada bundel dan buat perubahan yang Anda inginkan. Misalnya, Anda dapat menerapkan sistem operasi terbaru dan patch aplikasi lalu menginstal aplikasi tambahan.

   Atau, Anda dapat membuat yang baru WorkSpace dengan paket perangkat lunak dasar yang sama (Plus atau Standar) sebagai gambar yang digunakan untuk membuat bundel, dan membuat perubahan.
2. Jika Anda masih terhubung ke WorkSpace, putuskan sambungan dengan memilih Amazon WorkSpaces dan Putuskan sambungan di aplikasi WorkSpaces klien.

3. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
4. Di panel navigasi, pilih WorkSpaces.
5. Pilih WorkSpace dan pilih Tindakan, Buat Gambar. Jika statusnya`STOPPED`, Anda harus memulainya terlebih dahulu (pilih Actions, Start WorkSpaces) sebelum Anda dapat memilih Actions, Create Image. WorkSpace
6. Masukkan sebuah nama dan deskripsi untuk citra lalu pilih Buat citra. WorkSpace Tidak tersedia saat gambar sedang dibuat. Untuk detail informasi tentang proses pembuatan citra, lihat Buat WorkSpaces gambar dan bundel khusus.
7. Di panel navigasi, pilih Paket.
8. Pilih paket untuk membuka halaman detail, lalu di bagian Citra sumber, pilih Edit.
9. Pada halaman Perbarui citra sumber, pilih citra yang Anda buat dan pilih Paket pembaruan.
10. Jika diperlukan, perbarui WorkSpaces yang ada yang didasarkan pada bundel dengan membangun kembali WorkSpaces atau menghapus dan membuatnya kembali. Untuk informasi selengkapnya, lihat Membangun kembali WorkSpace.

Untuk memperbarui paket pemrograman

Untuk membuat paket secara terprogram, gunakan Tindakan API UpdateWorkspaceBundle. Untuk informasi selengkapnya, lihat UpdateWorkspaceBundledi Referensi WorkSpaces API Amazon.

Salin WorkSpaces gambar khusus

Anda dapat menyalin WorkSpaces gambar kustom di dalam atau di seluruh AWS Wilayah. Menyalin hasil citra dalam pembuatan citra identik dengan pengenal uniknya.

Anda dapat menyalin Bawa Lisensi Anda Sendiri (BYOL) ke Wilayah lain selama Wilayah tujuan diaktifkan untuk BYOL. Pastikan BYOL diaktifkan untuk semua akun dan Wilayah yang terlibat.

> **Note**
>
> Di Wilayah China (Ningxia), Anda dapat menyalin citra hanya di Wilayah yang sama.
> Di AWS GovCloud (US) Region s, untuk menyalin gambar ke dan dari AWS Wilayah lain, hubungi AWS Support.
> Di Wilayah Keikutsertaan, untuk menyalin gambar ke Wilayah lain, hubungi AWS Support. Untuk informasi selengkapnya tentang Wilayah Keikutsertaan, lihat Wilayah yang Tersedia.

Anda juga dapat menyalin citra yang telah dibagikan dengan Anda oleh Akun AWS lainnya. Untuk informasi selengkapnya tentang citra dasar, lihat Bagikan atau batalkan berbagi gambar kustom WorkSpaces .

Tidak ada biaya tambahan untuk menyalin citra di dalam atau lintas Wilayah. Namun, kuota untuk jumlah citra di Wilayah tujuan berlaku. Untuk informasi selengkapnya tentang WorkSpaces kuota Amazon, lihat WorkSpaces Kuota Amazon.

Izin IAM untuk menyalin citra

Jika Anda menggunakan pengguna IAM untuk menyalin citra, pengguna harus memiliki izin untuk `workspaces:DescribeWorkspaceImages` dan `workspaces:CopyWorkspaceImage`.

Contoh kebijakan berikut memungkinkan pengguna menyalin citra tertentu ke akun tertentu di Wilayah tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

Jika Anda membuat kebijakan IAM untuk menyalin citra yang dibagikan untuk akun yang tidak memiliki citra, Anda tidak dapat menentukan ID akun di ARN. Sebaliknya, Anda harus menggunakan * untuk ID akun, seperti yang ditunjukkan dalam kebijakan contoh berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Anda dapat menentukan ID akun di ARN hanya ketika akun tersebut memiliki citra yang akan disalin.

Untuk informasi lebih lanjut tentang bekerja dengan pengguna IAM, lihat Identitas dan manajemen akses untuk WorkSpaces.

Salin gambar massal

Anda dapat menyalin satu per satu citra menggunakan konsol tersebut. Untuk menyalin citra massal, gunakan Operasi API CopyWorkspaceImage atau perintah copy-workspace-image di AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat CopyWorkspaceImagedi Referensi Amazon WorkSpaces API atau lihat copy-workspace-imagedi Referensi AWS CLI Perintah.

Important

Sebelum menyalin citra yang dibagikan, pastikan untuk memverifikasi bahwa citra tersebut telah dibagikan dari Akun AWS. Untuk menentukan apakah gambar telah dibagikan dan untuk melihat ID AWS akun yang memiliki gambar, gunakan operasi DescribeWorkSpaceImagesdan DescribeWorkspaceImagePermissionsAPI atau describe-workspace-image-permissionsperintah describe-workspace-imagesand diAWS CLI.

Untuk menyalin citra menggunakan konsol tersebut

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.

2. Di panel navigasi, pilih Citra.
3. Pilih citra dan pilih Tindakan, Salin citra.
4. Untuk Pilih tujuan, pilih Wilayah AWS tempat Anda ingin meletakkan salinan citra.
5. UntukNama salinan, masukkan nama baru untuk citra yang disalin, dan untuk Deskripsi, masukkan deskripsi untuk citra yang disalin.
6. (Opsional) Di bagian Tanda, masukkan tanda untuk citra yang disalin. Untuk informasi selengkapnya, lihat WorkSpaces Sumber daya tag.
7. Pilih Salin citra.

Bagikan atau batalkan berbagi gambar kustom WorkSpaces

Anda dapat membagikan WorkSpaces gambar kustom di seluruh AWS akun dalam AWS Wilayah yang sama. Setelah citra dibagikan, akun penerima dapat menyalin citra ke Wilayah AWS seperlunya. Untuk informasi selengkapnya tentang menyalin objek, lihat Salin WorkSpaces gambar khusus.

> **Note**
>
> Di Wilayah China (Ningxia), Anda dapat menyalin citra hanya di Wilayah yang sama.
> Di AWS GovCloud (US) Region s, untuk menyalin gambar ke dan dari AWS Wilayah lain, hubungi AWS Support.

Tidak ada biaya tambahan untuk membagikan citra. Namun, kuota untuk jumlah citra di Wilayah AWS berlaku. Citra yang dibagikan tidak dihitung terhadap kuota akun penerima hingga penerima menyalin citra. Untuk informasi selengkapnya tentang WorkSpaces kuota Amazon, lihat WorkSpaces Kuota Amazon.

Untuk menghapus citra yang dibagikan, Anda harus membatalkan pembagian citra sebelum dapat menghapusnya.

Bagikan citra Bawa Lisensi Anda Sendiri

Anda dapat membagikan citra Bawa Lisensi Anda Sendiri (BYOL) hanya dengan akun AWS yang diaktifkan untuk BYOL. Akun AWS tempat Anda ingin membagikan citra BYOL juga harus menjadi bagian dari organisasi Anda (di bagian akun pembayar yang sama).

> **Note**
>
> Berbagi gambar BYOL di seluruh AWS akun saat ini tidak didukung di Wilayah AWS GovCloud (AS-Barat) dan AWS GovCloud (AS-Timur). Untuk berbagi gambar BYOL di seluruh akun di Wilayah AWS GovCloud (AS-Barat) dan AWS GovCloud (AS-Timur), hubungi Support. AWS

Citra yang dibagikan dengan Anda

Jika citra dibagikan dengan Anda, Anda dapat menyalinnya. Anda kemudian dapat menggunakan salinan gambar yang dibagikan untuk membuat bundel untuk meluncurkan yang baru WorkSpaces.

> **Important**
>
> Sebelum menyalin citra yang dibagikan, pastikan untuk memverifikasi bahwa citra tersebut telah dibagikan dari Akun AWS. Untuk menentukan secara terprogram apakah gambar telah dibagikan, gunakan operasi DescribeWorkSpaceImagesdan DescribeWorkspaceImagePermissionsAPI atau describe-workspace-image-permissionsperintah describe-workspace-imagesdan di antarmuka baris AWS perintah (CLI).

Tanggal pembuatan yang ditampilkan untuk citra yang telah dibagikan dengan Anda adalah tanggal citra dibuat pertama kali, bukan tanggal citra dibagikan dengan Anda.

Jika citra telah dibagikan dengan Anda, Anda tidak dapat membagikannya lebih jauh ke akun lain.

Untuk membagikan citra

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Citra.
3. Pilih citra untuk membuka halaman detailnya.
4. Pada halaman detail citra, di bagian Akun bersama, pilih Tambah akun.
5. Pada halaman Tambah akun, di bagian Tambahkan akun untuk dibagikan, masukkan ID akun dari akun tempat Anda ingin membagikan citra.

> **Important**
>
> Sebelum membagikan citra, konfirmasikan bahwa Anda membagikan dengan ID akun AWS.

6. Pilih Bagikan citra.

> **Note**
>
> Untuk menggunakan citra yang dibagikan, akun penerima harus menyalin citra terlebih dahulu. Akun penerima kemudian dapat menggunakan salinan gambar bersama untuk membuat bundel untuk meluncurkan yang baru WorkSpaces.

Untuk berhenti membagikan citra

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Citra.
3. Pilih citra untuk membuka halaman detailnya.
4. Pada halaman detail citra, di bagian Akun yang dibagikan, pilih akun AWS tempat Anda ingin berhenti membagikan citra, lalu pilih Batalkan Pembagian.
5. Saat diminta mengonfirmasi pembatalan pembagian citra, pilih Batalkan Pembagian.

> **Note**
>
> Jika Anda ingin menghapus citra setelah membatalkan pembagiannya, Anda harus terlebih dahulu membatalkan pembagiannya dari semua akun yang telah dibagikan.

Setelah Anda berhenti membagikan citra, akun penerima tidak dapat lagi membuat salinan citra. Namun, salinan gambar bersama yang sudah ada di akun penerima tetap ada di akun itu, dan baru WorkSpaces dapat diluncurkan dari salinan tersebut.

Untuk membagikan atau membatalkan pembagian citra secara terprogram

Untuk berbagi atau membatalkan berbagi gambar secara terprogram, gunakan operasi UpdateWorkspaceImagePermissionAPI atau perintah update-workspace-image-permissionAWS

Command Line Interface()AWS CLI. Untuk menentukan apakah gambar telah dibagikan, gunakan operasi DescribeWorkspaceImagePermissionsAPI atau perintah describe-workspace-image-permissionsCLI.

Hapus WorkSpaces bundel atau gambar khusus

Anda dapat menghapus paket kustom atau citra kustom yang tidak terpakai sesuai kebutuhan.

Hapus paket

Untuk menghapus bundel, Anda harus terlebih dahulu menghapus semua WorkSpaces yang didasarkan pada bundel.

Untuk menghapus paket menggunakan konsol

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Paket.
3. Pilih paket dan pilih Hapus.
4. Saat diminta konfirmasi, pilih Hapus.

Untuk menghapus paket secara terprogram

Untuk membuat paket secara terprogram, gunakan Tindakan API DeleteWorkspaceBundle. Untuk informasi selengkapnya, lihat DeleteWorkspaceBundledi Referensi Amazon WorkSpaces API.

> **Note**
>
> Pastikan Anda menunggu setidaknya 2 jam setelah menghapus bundel sebelum membuat bundel baru dengan nama yang sama.

Hapus citra

Setelah Anda menghapus paket kustom, Anda dapat menghapus citra yang Anda gunakan untuk membuat atau memperbarui paket.

Untuk menghapus citra, Anda harus terlebih dahulu menghapus setiap paket yang terkait dengan citra atau memperbarui paket tersebut untuk menggunakan citra sumber lain. Anda juga harus

membatalkan pembagian citra jika dibagikan dengan akun lain. Citra juga tidak dapat berada dalam status Tertunda atau Memvalidasi.

Untuk menghapus citra menggunakan konsol tersebut

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Citra.
3. Pilih citra lalu pilih Hapus.
4. Saat diminta konfirmasi, pilih Hapus.

Untuk menghapus citra secara terprogram

Untuk menghapus citra secara terprogram, gunakan Tindakan API DeleteWorkspaceImage. Untuk informasi selengkapnya, lihat DeleteWorkspaceImagedi Referensi Amazon WorkSpaces API.

Bawa lisensi desktop Windows Anda sendiri

Jika perjanjian lisensi Anda dengan Microsoft mengizinkannya, Anda dapat membawa dan menyebarkan desktop Windows 10 atau 11 Anda di desktop Anda. WorkSpaces Untuk melakukan ini, Anda harus mengaktifkan Bring Your Own License (BYOL) dan memberikan lisensi Windows 10 atau 11 yang memenuhi persyaratan di bawah ini. Untuk informasi selengkapnya tentang penggunaan perangkat lunak Microsoft AWS, lihat Amazon Web Services dan Microsoft.

Agar tetap mematuhi persyaratan lisensi Microsoft, AWS jalankan BYOL Anda WorkSpaces pada perangkat keras yang didedikasikan untuk Anda di Cloud. AWS Dengan membawa lisensi Anda sendiri, Anda dapat menyediakan pengalaman yang konsisten bagi pengguna. Untuk informasi lebih lanjut, lihat WorkSpaces Harga.

> **Important**
>
> Pembuatan gambar tidak didukung pada sistem Windows 10 atau 11 yang telah ditingkatkan dari satu versi Windows 10 atau 11 ke versi Windows 10 atau 11 yang lebih baru (peningkatan fitur/versi Windows). Namun, pembaruan kumulatif atau keamanan Windows didukung oleh proses pembuatan WorkSpaces gambar.

Daftar Isi

Persyaratan

Sebelum memulai, lakukan hal berikut:

- Perjanjian lisensi Microsoft Anda memungkinkan Windows berjalan di lingkungan yang dihosting virtual.
- Jika Anda akan menggunakan bundel non-GPU (bundel selain Graphics.g4dn, .g4dn, Graphics, dan), GraphicsPro verifikasi bahwa Anda akan menggunakan minimal 100 per Wilayah. GraphicsPro WorkSpaces 100 ini WorkSpaces dapat berupa campuran dari AlwaysOn dan AutoStop WorkSpaces. Menggunakan minimal 100 WorkSpaces per Wilayah adalah persyaratan untuk menjalankan perangkat WorkSpaces keras khusus Anda. Menjalankan perangkat keras khusus Anda WorkSpaces diperlukan untuk mematuhi persyaratan lisensi Microsoft. Perangkat keras khusus disediakan di AWS samping, sehingga VPC Anda dapat tetap pada penyewaan default.

  Jika Anda berencana untuk menggunakan bundel berkemampuan GPU (Graphics.g4dn, GraphicsPro .g4dn, Graphics, and GraphicsPro), verifikasi bahwa Anda akan menjalankan minimal 4 atau 20 GPU yang diaktifkan di Wilayah per bulan pada perangkat keras khusus. AlwaysOn AutoStop WorkSpaces

> **Note**
>
> - Graphics.g4dn, GraphicsPro .g4dn, Graphics, dan GraphicsPro bundel hanya dapat dibuat untuk protokol PCoIP saat ini.
> - Bundel grafis tidak lagi didukung setelah 30 November 2023. Kami merekomendasikan untuk memigrasikan paket Anda WorkSpaces ke Graphics.g4dn. Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.
> - Grafik dan GraphicsPro bundel saat ini tidak tersedia di Wilayah Asia Pasifik (Mumbai).
> - Graphics.g4dn, GraphicsPro .g4dn, Grafik, dan GraphicsPro bundel saat ini tidak tersedia di Wilayah Afrika (Cape Town).
> - Untuk menjalankan Anda WorkSpaces di Wilayah Afrika (Cape Town), Anda diminta untuk menjalankan minimal 400 WorkSpaces di Wilayah Afrika (Cape Town).
> - Bundel Windows 11 hanya dapat dibuat untuk protokol WSP.
> - Bundel Graphics.g4dn dan GraphicsPro .g4dn saat ini tidak tersedia untuk Windows 11.
> - Grafik dan GraphicsPro bundel tidak didukung untuk Windows 11.
> - Paket nilai tidak tersedia untuk Windows 11. Untuk informasi selengkapnya tentang memigrasi paket nilai yang ada, WorkSpaces lihatMigrasi a WorkSpace.
> - Untuk pengalaman konferensi video terbaik, kami sarankan menggunakan Power atau bundel PowerPro

- WorkSpaces dapat menggunakan antarmuka manajemen dalam rentang alamat IP /16. Antarmuka manajemen terhubung ke jaringan WorkSpaces manajemen aman yang digunakan untuk streaming interaktif. Ini memungkinkan WorkSpaces untuk mengelola Anda WorkSpaces. Untuk informasi selengkapnya, lihat Antarmuka jaringan. Anda harus menyimpan /16 netmask setidaknya dari salah satu rentang alamat IP berikut untuk tujuan ini:
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 198.18.0.0/15

> **Note**
>
> - Saat Anda mengadopsi WorkSpaces layanan, rentang alamat IP antarmuka manajemen yang tersedia sering berubah. Untuk menentukan rentang mana yang saat ini tersedia, jalankan perintah list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI).
> - Selain blok CIDR /16 yang Anda pilih, rentang alamat IP 54.239.224.0/20 digunakan untuk lalu lintas antarmuka manajemen di semua Wilayah. AWS

- Pastikan Anda telah membuka port antarmuka manajemen yang diperlukan untuk aktivasi Microsoft Windows dan Microsoft Office KMS untuk WorkSpaces BYOL. Untuk informasi selengkapnya, lihat Port antarmuka manajemen.
- Anda memiliki mesin virtual (VM) yang menjalankan Windows versi 64-bit yang didukung. Untuk daftar versi yang didukung, lihat bagian berikutnya dalam topik ini, Versi Windows yang didukung untuk BYOL. VM juga harus memenuhi persyaratan berikut:
  - Sistem operasi Windows harus diaktifkan terhadap server manajemen kunci Anda.
  - Sistem operasi Windows harus menjadikan English (United States) sebagai bahasa utamanya.
  - Selain perangkat lunak yang telah disertakan dengan Windows tidak dapat diinstal di VM. Anda dapat menambahkan perangkat lunak tambahan seperti solusi antivirus jika nanti Anda membuat citra kustom.
  - Jangan menyesuaikan profil pengguna default (`C:\Users\Default`) atau membuat penyesuaian lainnya sebelum membuat citra. Semua penyesuaian harus dibuat setelah pembuatan citra. Kami merekomendasikan untuk melakukan penyesuaian terhadap profil pengguna melalui Group Policy Objects (GPO) dan menerapkannya setelah pembuatan citra. Karena penyesuaian yang dilakukan melalui GPO dapat dengan mudah diubah atau dikembalikan dan tidak rentan terhadap kesalahan penyesuaian yang ditetapkan pada profil pengguna default.
  - Anda harus membuat akun WorkSpaces_BYOL dengan akses administrator lokal sebelum Anda membagikan gambar. Sebaiknya Anda mencatat kata sandi untuk akun ini karena mungkin diperlukan nantinya.
  - VM harus berada pada volume tunggal dengan ukuran maksimum 70 GB dan setidaknya 10 GB ruang kosong. Jika Anda berencana berlangganan Microsoft Office untuk citra BYOL Anda, VM harus berada pada volume tanggal dengan ukuran maksimum 70 GB dan setidaknya 20 GB ruang kosong. DISK tempat volume root aktif tidak boleh melebihi 70GB.

  - VM Anda harus menjalankan Windows PowerShell versi 4 atau yang lebih baru.
- Pastikan Anda telah menginstal patch Microsoft Windows terbaru sebelum menjalankan skrip pemeriksa BYOL di Langkah 3: Jalankan PowerShell skrip BYOL Checker pada Windows VM.

> **Note**
>
> - Untuk BYOL AutoStop WorkSpaces, sejumlah besar login bersamaan dapat menghasilkan peningkatan waktu yang signifikan WorkSpaces untuk tersedia. Jika Anda mengharapkan banyak pengguna untuk masuk ke BYOL Anda AutoStop WorkSpaces pada saat yang sama, silakan berkonsultasi dengan manajer akun Anda untuk saran.
> - AMI terenkripsi tidak didukung dalam proses pengimporan. Pastikan Anda menonaktifkan instans yang digunakan untuk membuat EC2 AMI memiliki enkripsi EBS. Enkripsi dapat diaktifkan setelah final WorkSpaces disediakan.

Versi Windows yang didukung untuk BYOL

VM Anda harus menjalankan salah satu dari versi Windows berikut ini:

- Windows 10 Versi 21H2 (Pembaruan Desember 2021)
- Windows 10 Versi 22H2 (Pembaruan November 2022)
- Windows 10 Perusahaan LTSC 2019 (1809)
- Windows 10 Perusahaan LTSC 2021 (21H2)
- Windows 11 Versi 23H2 (rilis Oktober 2023)
- Windows 11 Versi 22H2 (rilis Oktober 2022)

Semua versi OS yang didukung mendukung semua jenis komputasi yang tersedia di AWS Wilayah tempat Anda menggunakan WorkSpaces. Versi Windows yang tidak lagi didukung oleh Microsoft tidak dijamin berfungsi dan tidak didukung oleh AWS Support.

> **Note**
>
> Versi Windows 10 N dan Windows 11 N tidak didukung untuk BYOL saat ini.

Tambahkan Microsoft Office untuk citra BYOL

Jika Anda memilih untuk berlangganan Office melalui AWS, biaya tambahan akan berlaku. Untuk informasi lebih lanjut, lihat WorkSpaces Harga.

Important

- Jika Microsoft Office sudah diinstal pada VM yang Anda gunakan untuk membuat gambar BYOL Anda, Anda harus menghapus instalannya dari VM jika Anda ingin berlangganan Office melalui. AWS
- Jika Anda berencana untuk berlangganan Office melalui AWS, pastikan VM Anda memiliki setidaknya 20 GB ruang disk kosong.
- Selama impor gambar, Anda dapat berlangganan Office 2016 atau 2019 tetapi tidak ke Office 2021. Untuk Office 2021 dan aplikasi lain seperti Microsoft Visio 2021 dan Microsoft Project 2021, lihat Mengelola aplikasi.
- Untuk membawa lisensi Microsoft 365 Anda sendiri untuk aplikasi berbasis browser dan desktop di Amazon, WorkSpaces instal aplikasi Microsoft 365 pada gambar BYOL Anda setelah proses pengambilan gambar BYOL selesai.

Note

Gambar Graphics.g4dn GraphicsPro dan.g4dn BYOL hanya mendukung Office 2019 dan tidak mendukung Office 2016.

Jika Anda memilih berlangganan Office, proses penyerapan citra BYOL memerlukan waktu setidaknya 3 jam.

Untuk detail tentang berlangganan Office saat proses penyerapan BYOL, lihat Langkah 6: Buat gambar BYOL menggunakan konsol WorkSpaces .

Pengaturan bahasa Office

Kami memilih bahasa yang digunakan untuk langganan Office Anda berdasarkan AWS Wilayah tempat Anda melakukan pengambilan gambar BYOL Anda. Misalnya, jika Anda melakukan penyerapan citra BYOL di Wilayah Asia Pacific (Tokyo), langganan Office Anda memiliki bahasa Jepang sebagai bahasanya.

Secara default, kami menginstal sejumlah paket bahasa Office yang sering digunakan pada Anda WorkSpaces. Jika paket bahasa yang Anda inginkan tidak terinstal, Anda dapat mengunduh paket bahasa tambahan dari Microsoft. Untuk informasi selengkapnya, lihat Paket Aksesori Bahasa untuk Office dalam dokumentasi Microsoft.

Untuk mengubah bahasa untuk Office, Anda memiliki beberapa opsi:

Opsi 1: Mengizinkan pengguna individu menyesuaikan pengaturan bahasa Office mereka

Pengguna individu dapat menyesuaikan pengaturan bahasa Office pada mereka WorkSpaces. Untuk informasi selengkapnya, lihat Tambahkan bahasa pengeditan atau penulisan atau tetapkan preferensi bahasa di Office dalam dokumentasi Microsoft.

Opsi 2: Gunakan templat administratif GPO (.admx/.adl) untuk menerapkan pengaturan bahasa Office default untuk semua pengguna Anda WorkSpaces

Anda dapat menggunakan pengaturan Objek Kebijakan Grup (GPO) untuk menerapkan pengaturan bahasa Office default bagi pengguna Anda WorkSpaces .

> **Note**
>
> WorkSpaces Pengguna Anda tidak akan dapat mengganti pengaturan bahasa yang diberlakukan melalui GPO.

Untuk informasi selengkapnya tentang penggunaan GPO untuk mengatur bahasa untuk Office, lihat Penyiapan dan pengaturan bahasa Kustom untuk Office dalam dokumentasi Microsoft. Office 2016 dan Office 2019 menggunakan pengaturan GPO yang sama (diberi label Office 2016).

Untuk bekerja dengan GPO, Anda harus menginstal alat administrasi Direktori Aktif. Untuk informasi penggunaan alat administrasi Direktori Aktif untuk digunakan dengan GPO, lihat Siapkan Alat Administrasi Direktori Aktif untuk WorkSpaces.

Sebelum Anda dapat mengonfigurasi pengaturan kebijakan Office 2016 atau Office 2019, Anda harus mengunduh file templat administratif (.admx/.adl) untuk Office dari Pusat Unduhan Microsoft. Setelah Anda mengunduh file template administratif, Anda harus menambahkan `office16.adml` file `office16.admx` dan ke Central Store dari pengontrol domain untuk WorkSpaces direktori Anda. (file `office16.admx` dan `office16.adml` yang berlaku untuk Office 2016 dan Office 2019.) Untuk informasi lebih lanjut tentang bekerja dengan file `.admx` dan `.adml`, lihat Cara membuat

dan mengelola Pusat Penyimpanan untuk Templat Administratif Kebijakan Grup di Windows dalam dokumentasi Microsoft.

Prosedur berikut menjelaskan cara membuat Pusat Penyimpanan dan menambahkan file templat administratif. Lakukan prosedur berikut pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke direktori Anda WorkSpaces .

Untuk menginstal file templat administratif Kebijakan Grup untuk Office

1. Unduh file templat administratif (.admx/.adl) untuk Office dari Pusat Unduhan Microsoft.
2. Pada administrasi direktori WorkSpace atau instans Amazon EC2 yang digabungkan ke WorkSpaces direktori Anda, buka Windows File Explorer, dan di bilah alamat, masukkan nama domain yang memenuhi syarat penuh (FQDN) organisasi Anda, seperti. `\\example.com`
3. Buka folder `SYSVOL`.
4. Buka folder dengan nama *`FQDN`*.
5. Buka folder `Policies`. Anda sekarang seharusnya berada di `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies`.
6. Jika belum ada, buat folder dengan nama `PolicyDefinitions`.
7. Buka folder `PolicyDefinitions`.
8. Salin file `office16.admx` ke dalam folder `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions`.
9. Buat folder dengan nama `en-US` di dalam folder `PolicyDefinitions`.
10. Buka folder `en-US`.
11. Salin file `office16.adml` ke folder `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions\en-US`.

Untuk mengonfigurasi pengaturan bahasa GPO untuk Office

1. Pada administrasi direktori Anda WorkSpace atau instans Amazon EC2 yang bergabung ke WorkSpaces direktori Anda, buka alat Manajemen Kebijakan Grup ()gpmc.msc.
2. Perluas forest (Forest:***FQDN***).
3. Perluas Domain.
4. Perluas FQDN Anda (misalnya, `example.com`).
5. Pilih FQDN Anda, buka menu konteks (klik kanan) atau buka menu Tindakan, dan pilih Buat GPO di domain ini, dan Tautkan ke sini.

6. Beri nama GPO Anda (misalnya, **`Office`**).
7. Pilih GPO Anda, buka menu konteks (klik kanan) atau buka menu Tindakan, dan pilih Edit.
8. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi Pengguna, Kebijakan, Penetapan kebijakan Templat Administratif (file ADMX) diambil dari komputer lokal, Microsoft Office 2016, dan Preferensi Bahasa.

   > **Note**
   >
   > Office 2016 dan Office 2019 menggunakan pengaturan GPO yang sama (diberi label Office 2016). Jika Anda tidak melihat Penetapan Kebijakan Templat Administratif (file ADMX) diambil dari komputer lokal di Konfigurasi Pengguna, Kebijakan, file `office16.admx` dan `office16.adml` tidak diinstal dengan benar pada pengendali domain Anda.

9. Di bagian Preferensi Bahasa, tentukan bahasa yang ingin Anda terapkan untuk pengaturan berikut. Pastikan Anda menetapkan setiap pengaturan ke Diaktifkan, lalu di bagian Opsi, pilih bahasa yang Anda inginkan. Pilih OKE untuk menyimpan setiap pengaturan.

   - Bahasa Tampilan > Tampilkan bantuan di
   - Bahasa tampilan > Tampilkan menu dan kotak dialog di
   - Bahasa pengeditan > Bahasa Pengeditan Utama

10. Tutup alat Manajemen Kebijakan Grup jika Anda telah selesai.
11. Perubahan pengaturan Kebijakan Grup berlaku setelah pembaruan Kebijakan Grup berikutnya untuk WorkSpace dan setelah WorkSpace sesi dimulai ulang. Untuk menerapkan perubahan Kebijakan Grup, lakukan salah satu hal berikut:

    - Reboot WorkSpace (di WorkSpaces konsol Amazon, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
    - Dari prompt perintah administratif, masukkan gpupdate /force.

Opsi 3: Perbarui pengaturan registri bahasa Office di WorkSpaces

Untuk menetapkan pengaturan bahasa Office melalui registri, perbarui pengaturan pendaftaran berikut:

- HKEY_CURRENT_USER\ PERANGKAT LUNAK\ Microsoft\ Office\ 16.0\ Umum\\ UILanguage LanguageResources

- HKEY_CURRENT_USER\ PERANGKAT LUNAK\ Microsoft\ Office\ 16.0\ Umum\\ LanguageResources HelpLanguage

Untuk pengaturan ini, tambahkan nilai kunci DWORD dengan ID lokal Office (LCID) yang sesuai. Misalnya, LCID untuk English (US) adalah 1033. Karena LCID bernilai desimal, Anda harus mengatur Opsi dasar nilai DWORD ke Desimal. Untuk daftar LCID Office, lihat Pengenal bahasa dan nilai OptionState Id di Office 2016 di dokumentasi Microsoft.

Anda dapat menerapkan pengaturan registri ini ke pengaturan WorkSpaces GPO Anda atau skrip logon.

Untuk informasi lebih lanjut tentang bekerja dengan pengaturan bahasa untuk Office, lihat Penyiapan dan pengaturan bahasa kustom untuk Office dalam dokumentasi Microsoft.

Tambahkan Office ke BYOL Anda yang ada WorkSpaces

Anda juga dapat menambahkan langganan Office ke BYOL Anda yang ada WorkSpaces dengan melakukan hal berikut.

- Kelola aplikasi (disarankan) - Anda dapat menginstal dan mengonfigurasi Microsoft Office, Microsoft Visio, atau Microsoft Project 2021 yang sudah ada. WorkSpaces Untuk informasi selengkapnya, lihat Mengelola aplikasi.
- Memigrasi WorkSpace - Setelah membuat bundel BYOL dengan Office terinstal, Anda dapat menggunakan fitur WorkSpaces migrasi untuk memigrasikan BYOL yang ada WorkSpaces ke bundel BYOL yang berlangganan Office. Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.

> **Note**
>
> Opsi kelola aplikasi tersedia untuk menginstal Microsoft Office 2021 dan aplikasi lain, seperti Microsoft Visio 2021 dan Microsoft Project 2021 ke aplikasi Anda. WorkSpaces Untuk menginstal Microsoft Office 2016 atau 2019 pada Anda WorkSpaces, gunakanMigrasi a WorkSpace.

Migrasi antar versi Microsoft Office

Untuk bermigrasi dari satu versi Microsoft Office ke versi lain, Anda memiliki opsi berikut:

- Kelola aplikasi (disarankan) — Anda dapat menghapus instalan versi Office asli dan menginstal Office 2021 dan aplikasi lain, seperti Microsoft Visio 2021 dan Microsoft Project 2021, di aplikasi yang sudah ada. WorkSpaces Misalnya, untuk bermigrasi dari Microsoft Office 2019 ke Microsoft Office 2021, gunakan alur kerja kelola aplikasi untuk menghapus instalan Microsoft Office 2019 dan menginstal Microsoft Office 2021. Untuk informasi selengkapnya, lihat Mengelola aplikasi.
- Memigrasi WorkSpace - Untuk bermigrasi dari Microsoft Office 2016 ke 2019 atau dari Microsoft Office 2019 ke 2016, Anda harus membuat bundel BYOL yang berlangganan versi Office yang ingin Anda migrasi. Kemudian, gunakan fitur WorkSpaces migrasi untuk memigrasikan BYOL WorkSpaces yang sudah ada yang berlangganan Office ke bundel BYOL yang berlangganan versi Office yang ingin Anda migrasi. Misalnya, untuk bermigrasi dari Office 2016 ke 2019, buat bundel BYOL yang berlangganan Office 2019. Kemudian gunakan fitur WorkSpaces migrasi untuk memigrasi BYOL yang sudah ada WorkSpaces yang berlangganan Office 2016 ke bundel BYOL yang berlangganan Office 2019. Untuk informasi selengkapnya, lihat Memigrasi a. WorkSpace

Anda dapat menggunakan opsi ini untuk memigrasi Anda WorkSpaces yang berlangganan Microsoft Office melalui aplikasi AWS Microsoft 365. Namun, mengelola aplikasi terbatas untuk menghapus instalan Microsoft Office dari Anda WorkSpace. Anda harus membawa alat dan installer Anda sendiri untuk menginstal aplikasi Microsoft 365 di aplikasi Anda WorkSpaces.

> **Note**
>
> Dengan menggunakan kelola aplikasi, Anda dapat menginstal atau menghapus instalan Microsoft Office, Microsoft Visio, atau MicrosoftProject 2021 di aplikasi Anda. WorkSpaces Untuk versi Microsoft Office 2016 atau 2019, Anda hanya dapat menghapusnya dari versi Anda WorkSpaces. Untuk menginstal Microsoft Office 2016 atau 2019 pada Anda WorkSpaces, memigrasikan WorkSpace file.

Untuk informasi selengkapnya tentang proses migrasi, lihat Migrasi a WorkSpace.

Berhenti berlangganan dari Office

Untuk berhenti berlangganan dari Office, Anda memiliki opsi berikut.

- Kelola aplikasi (disarankan) - Anda dapat menghapus instalan Microsoft Office dan aplikasi lain seperti Microsoft Visio dan Microsoft Project dari aplikasi Anda. WorkSpaces Untuk informasi selengkapnya, lihat Mengelola aplikasi.

- Migrasi a WorkSpace - Anda dapat membuat bundel BYOL yang tidak berlangganan Office. Kemudian gunakan fitur WorkSpaces migrasi untuk memigrasikan BYOL Anda yang ada WorkSpaces ke bundel BYOL yang tidak berlangganan Office. Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.

Pembaruan Office

Jika Anda telah berlangganan Office melalui AWS, pembaruan Office disertakan sebagai bagian dari pembaruan Windows reguler Anda. Untuk memiliki patch dan pembaruan terkini, sebaiknya Anda memperbarui citra dasar BYOL secara berkala.

Langkah 1: Periksa kelayakan akun Anda untuk BYOL menggunakan konsol Amazon WorkSpaces

Sebelum Anda dapat mengaktifkan akun Anda untuk BYOL, Anda harus melalui proses verifikasi untuk mengonfirmasi kelayakan Anda untuk BYOL. Sampai Anda melalui proses ini, opsi Aktifkan BYOL tidak akan tersedia di WorkSpaces konsol Amazon Anda.

> **Note**
>
> Proses verifikasi memakan waktu setidaknya satu hari kerja dan dapat memakan waktu lebih lama jika Anda ingin menautkan dua atau lebih AWS akun yang mendukung BYOL bersama-sama sehingga mereka menggunakan perangkat keras dasar yang sama.

Untuk memeriksa kelayakan akun Anda untuk BYOL dengan menggunakan konsol Amazon WorkSpaces

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Pengaturan Akun, lalu di bawah Bawa lisensi Anda sendiri (BYOL), pilih Lihat pengaturan WorkSpaces BYOL. Jika akun Anda saat ini tidak memenuhi syarat untuk BYOL, suatu pesan menyediakan panduan untuk langkah selanjutnya. Untuk memulai, hubungi manajer AWS akun atau perwakilan penjualan Anda, atau hubungi AWS Support Pusat. Kontak Anda akan memverifikasi kelayakan Anda untuk BYOL.

   Untuk menentukan kelayakan Anda untuk BYOL, kontak Anda akan memerlukan informasi tertentu dari Anda. Misalnya, Anda mungkin diminta untuk menjawab pertanyaan berikut.

- Apakah Anda telah meninjau dan menerima daftar Persyaratan BYOL sebelumnya?
- Di AWS Wilayah mana Anda memerlukan akun Anda diaktifkan untuk BYOL?
- Berapa banyak BYOL yang WorkSpaces Anda rencanakan untuk disebarkan per Wilayah? AWS
- Apa rencana peningkatan Anda?
- Apakah Anda membeli WorkSpaces dari reseller?
- Apa tipe paket yang Anda butuhkan untuk BYOL?
- Apakah organisasi Anda memiliki AWS akun lain yang diaktifkan untuk BYOL di Wilayah yang sama? Jika ya, apakah Anda ingin menautkan akun ini agar menggunakan perangkat keras dasar yang sama?

  Jika akun ditautkan, jumlah total yang WorkSpaces digunakan dalam akun ini digabungkan bersama untuk tujuan menentukan kelayakan Anda untuk BYOL. Perhatikan bahwa menautkan akun membutuhkan waktu tambahan. Jika Anda ingin menautkan akun, Anda harus menyediakan jumlah akun ke kontak Anda.

3. Setelah kelayakan Anda dikonfirmasi untuk BYOL, Anda dapat melanjutkan ke langkah berikutnya, di mana Anda mengaktifkan BYOL untuk akun Anda di konsol Amazon. WorkSpaces

Langkah 2: Aktifkan BYOL untuk akun Anda untuk BYOL menggunakan konsol Amazon WorkSpaces

Untuk mengaktifkan BYOL untuk akun Anda, Anda harus menentukan antarmuka jaringan manajemen. Antarmuka ini terhubung ke jaringan WorkSpaces manajemen Amazon yang aman. Ini digunakan untuk streaming interaktif WorkSpace desktop ke WorkSpaces klien Amazon, dan untuk memungkinkan Amazon WorkSpaces mengelola WorkSpace.

> **Note**
>
> Anda hanya perlu melakukan langkah-langkah dalam prosedur ini sekali per Wilayah untuk mengaktifkan BYOL untuk akun Anda.

Untuk mengaktifkan BYOL untuk akun Anda dengan menggunakan konsol Amazon WorkSpaces

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.

2. Di panel navigasi, pilih Pengaturan Akun, lalu di bawah Bawa lisensi Anda sendiri (BYOL), pilih Lihat pengaturan WorkSpaces BYOL.
3. Di halaman Pengaturan Akun, di Bawa Lisensi Anda Sendiri (BYOL), pilih Aktifkan BYOL.

   Jika Anda tidak menemukan opsi Aktifkan BYOL, artinya akun Anda saat ini tidak layak untuk BYOL. Untuk informasi selengkapnya, lihat Langkah 1: Periksa kelayakan akun Anda untuk BYOL menggunakan konsol Amazon WorkSpaces .
4. Di Bawa Lisensi Anda Sendiri (BYOL), di area Rentang alamat IP antarmuka jaringan manajemen, pilih rentang alamat IP, lalu pilih Tampilkan blok CIDR yang tersedia.

   Amazon WorkSpaces mencari dan menampilkan rentang alamat IP yang tersedia sebagai blok IPv4 Classless Inter-Domain Routing (CIDR), dalam rentang yang Anda tentukan. Jika Anda memerlukan rentang alamat IP tertentu, Anda dapat mengedit rentang pencarian.

   > **Important**
   >
   > Setelah Anda menentukan rentang alamat IP, Anda tidak dapat memodifikasinya. Pastikan untuk menentukan rentang alamat IP yang tidak bertentangan dengan rentang yang digunakan oleh jaringan internal Anda. Jika Anda memiliki pertanyaan tentang rentang mana yang harus ditentukan, hubungi manajer AWS akun atau perwakilan penjualan Anda, atau hubungi AWS Support Pusat sebelum melanjutkan.
5. Pilih blok CIDR yang Anda inginkan dari daftar hasil, lalu pilih Aktifkan BYOL.

   Proses ini dapat memerlukan waktu beberapa jam. Saat WorkSpaces mengaktifkan akun Anda untuk BYOL, lanjutkan ke langkah berikutnya.

Langkah 3: Jalankan PowerShell skrip BYOL Checker pada Windows VM

Setelah Anda mengaktifkan BYOL untuk akun Anda, Anda harus mengonfirmasi bahwa VM Anda memenuhi persyaratan untuk BYOL. Untuk melakukannya, lakukan langkah-langkah ini untuk mengunduh dan menjalankan skrip Pemeriksa WorkSpaces PowerShell BYOL. Skrip melakukan serangkaian tes pada VM yang akan Anda gunakan untuk membuat citra Anda.

> **Important**
>
> VM harus lulus semua pengujian sebelum Anda dapat menggunakannya untuk BYOL.

Untuk mengunduh skrip Pemeriksa BYOL

Sebelum Anda mengunduh dan menjalankan skrip BYOL Checker, verifikasi bahwa pembaruan keamanan Windows terbaru diinstal pada VM Anda. Selagi skrip ini berjalan, proses menonaktifkan layanan Pembaruan Windows.

1. Unduh file .zip skrip Pemeriksa BYOL dari https://tools.amazonworkspaces.com/BYOLChecker.zip ke folder `Downloads` Anda.
2. Di folder `Downloads`, buat folder `BYOL`.
3. Ekstrak file dari `BYOLChecker.zip` dan salin ke folder `Downloads\BYOL`.
4. Hapus folder `Downloads\BYOLChecker.zip` sehingga hanya file yang diekstrak yang tersisa.

Lakukan langkah-langkah ini untuk menjalankan skrip Pemeriksa BYOL.

Untuk menjalankan skrip Pemeriksa BYOL

1. Dari desktop Windows, buka Windows PowerShell. Pilih tombol Start Windows, klik kanan Windows PowerShell, dan pilih Run as administrator. Jika Anda diminta oleh Kontrol Akun Pengguna untuk memilih apakah Anda PowerShell ingin membuat perubahan pada perangkat Anda, pilih Ya.
2. Pada prompt PowerShell perintah, ubah ke direktori tempat skrip Pemeriksa BYOL berada. Sebagai contoh, jika skrip terletak di `Downloads\BYOL`, masukkan perintah berikut lalu tekan Masukkan:

   ```
   cd C:\Users\username\Downloads\BYOL
   ```
3. Masukkan perintah berikut untuk memperbarui kebijakan PowerShell eksekusi di komputer. Melakukan hal ini memungkinkan skrip Pemeriksa BYOL untuk menjalankan:

   ```
   Set-ExecutionPolicy AllSigned
   ```
4. Ketika diminta untuk mengonfirmasi apakah akan mengubah kebijakan PowerShell eksekusi, masukkan A untuk menentukan Ya untuk Semua.
5. Masukkan perintah berikut untuk menjalankan skrip Pemeriksa BYOL:

   ```
   .\BYOLChecker.ps1
   ```
6. Jika notifikasi keamanan muncul, tekan tombol Runtuk menjalankan sekali.
7. Di kotak dialog Validasi WorkSpaces Gambar, pilih Mulai Tes.

8. Setelah menyelesaikan setiap tes, Anda dapat melihat status tes. Untuk setiap tes dengan status GAGAL, pilih Info Info untuk menampilkan informasi tentang cara menyelesaikan masalah yang menyebabkan kegagalan. Jika pengujian menampilkan status PERINGATAN, pilih tombol Perbaiki Semua Peringatan.
9. Jika berlaku, selesaikan masalah apa pun yang menyebabkan kegagalan pengujian dan peringatan, dan ulangi Step 7 dan Step 8 sampai VM lulus semua pengujian. Semua kegagalan dan peringatan harus diselesaikan sebelum Anda mengeskpor VM.
10. Pemeriksa skrip BYOL menghasilkan dua berkas log, `BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` dan `ImageInfo.text`. File ini terletak di direktori yang berisi file skrip Pemeriksa BYOL.

    > **Tip**
    >
    > Jangan hapus file berikut. Masalah yang terjadi mungkin dapat membantu pemecahan masalah.

11. Setelah VM Anda melewati semua pengujian, Anda mendapatkan pesan Validasi Berhasil. Tinjau pengaturan lokal VM yang ditampilkan di alat. Untuk memperbarui pengaturan lokal, ikuti Instruksi ini dalam dokumentasi Microsoft dan kembali menjalankan skrip pemeriksa BYOL.
12. Matikan VM dan buat snapshot.
13. Mulai VM lagi. Pilih Jalankan Sysprep. Jika Sysprep berhasil, VM yang Anda ekspor setelah Step 12dapat diimpor ke Amazon Elastic Compute Cloud (Amazon EC2). Jika tidak, tinjau log Sysprep, kembali ke snapshot yang diambil di Step 12, selesaikan masalah yang dilaporkan, ambil snapshot baru, dan kembali jalankan skrip Pemeriksa BYOL.

    Alasan kegagalan Sysprep yang paling umum adalah bahwa Paket Modern AppX tidak dihapus untuk semua pengguna. Gunakan Remove-AppxPackage PowerShell cmdlet untuk menghapus Paket AppX.
14. Setelah Anda berhasil membuat gambar Anda, Anda dapat menghapus akun WorkSpaces_BYOL.

Daftar pesan kesalahan dan perbaikan kesalahan

Impor BYOL membutuhkan Powershell 4.0 atau lebih tinggi. Versi yang diinstal PowerShell tidak didukung.

PowerShell versi 4.0 atau yang lebih baru harus diinstal. Untuk informasi selengkapnya, lihat Microsoft Windows PowerShell.

Impor BYOL tidak mendukung sistem dengan Microsoft Office aktif diinstal.

Microsoft Office harus dihapus instalasinya sebelum mengimpor. Untuk informasi selengkapnya, lihat Menghapus instalan Office dari PC.

Impor BYOL membutuhkan sistem tanpa Agen PCoIP.

Copot pemasangan Agen PCoIP. Untuk informasi tentang menghapus instalan agen PCoIP, lihat Menghapus instalasi Teradici PCoIP Software Client untuk Mac

Impor BYOL mengharuskan pembaruan Windows dinonaktifkan.

Nonaktifkan pembaruan Windows dengan mengikuti langkah-langkah berikut:

1. Tekan tombol Windows+R. Ketik`services.msc`, lalu tekan Enter.
2. Klik kanan pada Windows Update, lalu pilih Properties.
3. Di bawah tab Umum, atur jenis Startup ke Dinonaktifkan.
4. Pilih Berhenti.
5. Klik Terapkan, lalu pilih OK.
6. Mulai ulang komputer Anda.

Impor BYOL mengharuskan Automount diaktifkan.

Anda harus mengaktifkan Automount. Jalankan perintah berikut di PowerShell sebagai administrator.

```
C:\> diskpart
DISKPART> automount enable
```

Pemasangan otomatis volume baru diaktifkan.

Impor BYOL membutuhkan akun WorkSpaces _BYOL untuk diaktifkan

WorkSpacesAkun _BYOL harus diaktifkan. Untuk informasi selengkapnya, lihat Mengaktifkan BYOL untuk akun Anda untuk BYOL menggunakan konsol Amazon WorkSpaces .

Impor BYOL memerlukan antarmuka jaringan untuk menggunakan DHCP untuk secara otomatis menetapkan alamat IP. Antarmuka jaringan saat ini menggunakan alamat IP statis.

Antarmuka jaringan harus diubah untuk menggunakan DHCP. Untuk informasi selengkapnya, lihat Mengubah setelan TCP/IP.

Impor BYOL membutuhkan lebih dari 20 GB ruang pada disk lokal.

Disk lokal harus memiliki ruang yang cukup dan mengharuskan Anda membebaskan 20 GB atau lebih.

Impor BYOL membutuhkan sistem dengan 1 drive lokal. Ada tambahan Local, Removable atau Network drive.

Hanya drive C dan D yang dapat hadir pada WorkSpace yang digunakan untuk mengimpor gambar. Hapus semua drive lainnya, termasuk drive virtual.

Impor BYOL membutuhkan Windows 10 atau Windows 11.

Gunakan sistem operasi Windows 10 atau Windows 11.

Impor BYOL membutuhkan sistem yang tidak bergabung dengan domain AD.

Sistem harus tidak bergabung dari domain AD. Untuk informasi selengkapnya, lihat FAQ manajemen perangkat Azure Active Directory.

Impor BYOL membutuhkan sistem yang tidak bergabung dengan domain Azure.

Sistem harus tidak bergabung dari domain Azure. Untuk informasi selengkapnya, lihat FAQ manajemen perangkat Azure Active Directory.

Impor BYOL mengharuskan Windows Public Firewall dinonaktifkan.

Profil firewall publik harus dinonaktifkan. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan Microsoft Defender Firewall.

Impor BYOL membutuhkan sistem tanpa alat VMware.

Alat VMware harus dihapus instalasinya. Untuk informasi selengkapnya, lihat Menghapus instalasi dan menginstal VMware Tools secara manual di VMware Fusion (1014522).

Impor BYOL membutuhkan disk lokal kurang dari 80 GB.

Disk harus lebih kecil dari 80 GB. Kurangi ukuran disk.

Impor BYOL membutuhkan kurang dari 2 partisi pada drive lokal. Selain itu, semua partisi Windows 10 harus dipartisi MBR dan semua partisi Windows 11 harus dipartisi GPT.

Volume harus dipartisi MBR untuk Windows 10 dan GPT dipartisi untuk Windows 11. Untuk informasi selengkapnya, lihat Mengelola disk.

Impor BYOL mengharuskan semua pembaruan yang tertunda yang memerlukan reboot selesai.

Instal semua pembaruan dan reboot sistem operasi.

Impor BYOL mengharuskan AutoLogon dinonaktifkan.

Untuk menonaktifkan AutoLogon registri:

1. Tekan tombol Windows+R dan `Regedit.exe` ketik command prompt.
2. Gulir ke bawah ke `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`
3. Tambahkan nilai untuk`DontDisplayLastUserName`.
4. Untuk Tipe, masukkan`REG_SZ`.
5. Untuk Nilai, masukkan `0`.

> **Note**
>
> - Nilai `DontDisplayLastUserName` menentukan apakah kotak dialog logon menampilkan nama pengguna pengguna terakhir yang masuk ke PC.
> - Nilai tidak ada secara default. Jika ada, Anda harus mengaturnya ke `0` atau nilai `DefaultUser` akan dihapus dan AutoLogon akan gagal.

Impor BYOL **`RealTimeIsUniversal`** harus diaktifkan.

RealTimeUniversal Registry Key harus diaktifkan. Untuk informasi selengkapnya, lihat Mengkonfigurasi pengaturan waktu untuk Windows Server 2008 dan yang lebih baru.

Impor BYOL membutuhkan sistem dengan satu partisi yang dapat di-boot.

Jumlah partisi yang dapat di-boot tidak boleh melebihi satu.

Untuk menghapus partisi tambahan

1. Tekan logo Windows+R tombol untuk membuka kotak Run. Masuk `msconfig` dan tekan tombol Enter pada keyboard untuk membuka jendela Konfigurasi Sistem.
2. Pilih tab Boot dari jendela dan periksa apakah OS yang ingin Anda gunakan diatur ke OS saat ini; OS default. Jika tidak diatur, pilih OS yang Anda inginkan dari jendela dan pilih Set as default pada jendela yang sama.
3. Untuk menghapus partisi lain, pilih partisi itu, lalu pilih Hapus, Terapkan, OK.

Jika kesalahan masih muncul, boot komputer Anda dari disk instalasi atau perbaikan, dan ikuti langkah-langkah ini.

1. Lewati layar bahasa awal, lalu pilih Perbaiki komputer Anda di layar instal utama.
2. Pada layar Pilih opsi, pilih Troubleshoot.
3. Pada layar Opsi lanjutan, pilih Command Prompts.
4. Di command prompt, enter`bootrec.exe /fixmbr`, lalu tekan Enter.

Impor BYOL membutuhkan sistem 64 bit.

Gambar OS 64 bit harus digunakan. Untuk informasi selengkapnya, lihat Versi Windows yang didukung untuk BYOL.

Impor BYOL membutuhkan sistem yang belum dipersenjatai kembali.

Jumlah Image Rearm tidak boleh 0. Fitur persenjataan ulang memungkinkan Anda memperpanjang masa aktivasi untuk versi percobaan Windows. Proses Pembuatan Citra mengharuskan jumlah persenjataan ulang bernilai selain 0.

Untuk memeriksa jumlah persenjataan ulang Windows

1. Pada menu Start Windows, pilih Sistem Windows, lalu pilih Command Prompt.
2. Di Command Prompt`cscript C:\Windows\System32\slmgr.vbs /dlv`, masukkan, lalu tekan Enter.

3. Untuk mengatur ulang hitungan rearm ke nilai selain 0. Untuk informasi selengkapnya, lihat Sysprep (Generalisasi) instalasi Windows.

Impor BYOL membutuhkan sistem yang belum ditingkatkan di tempat. Sistem ini telah ditingkatkan di tempat.

Windows tidak boleh ditingkatkan dari versi sebelumnya.

Impor BYOL mengharuskan tidak ada antivirus yang diinstal pada sistem.

Anda harus menghapus instalasi perangkat lunak antivirus Anda. Jalankan olehOlChecker untuk mendapatkan detail untuk perangkat lunak antivirus untuk dihapus.

Impor BYOL membutuhkan sistem Windows 10 untuk memiliki mode Boot lama.

BIOS Legacy BootMode harus digunakan untuk Windows 10. Untuk informasi lebih lanjut, lihat Mode boot.

Langkah 4: Ekspor VM dari lingkungan virtualisasi Anda

Untuk membuat citra untuk BYOL, Anda harus terlebih dahulu mengekspor VM dari lingkungan virtualisasi Anda. VM harus berada pada volume tunggal dengan ukuran maksimum 70 GB dan setidaknya 10 GB ruang kosong. Untuk informasi lebih lanjut, lihat dokumentasi untuk lingkungan virtualisasi Anda dan Ekspor VM Anda dari Lingkungan Virtualisasi dalam Panduan pengguna VM Import/Export.

Langkah 5: Impor VM sebagai citra ke Amazon EC2

Setelah Anda mengekspor VM Anda, tinjau persyaratan untuk mengimpor sistem operasi Windows dari VM. Ambil tindakan sesuai kebutuhan. Untuk informasi selengkapnya, lihat Persyaratan Import/Export VM.

> **Note**
>
> Mengimpor VM dengan disk terenkripsi tidak didukung. Jika Anda memilih untuk enkripsi default untuk volume Amazon Elastic Block Store (Amazon EBS), Anda harus membatalkan pilihan tersebut sebelum mengimpor VM Anda.

Impor VM Anda ke Amazon EC2 sebagai Amazon Machine Image (AMI). Pilih salah satu metode berikut:

- Gunakan perintah import-image dengan AWS CLI. Untuk informasi lebih lanjut, lihat citra impor dalam Referensi Perintah AWS CLI .
- Gunakan Operasi API ImportImage. Untuk informasi selengkapnya, lihat ImportImagedi Referensi API Amazon EC2.

Untuk informasi selengkapnya, lihat Mengimpor VM sebagai Citra di Panduan Pengguna VM Import/Export.

Langkah 6: Buat gambar BYOL menggunakan konsol WorkSpaces

Lakukan langkah-langkah ini untuk membuat gambar WorkSpaces BYOL.

> **Note**
>
> Untuk melakukan prosedur ini, verifikasi bahwa Anda memiliki izin AWS Identity and Access Management (IAM) untuk:
>
> - Panggilan WorkSpaces **`ImportWorkspaceImage`**.
> - Hubungi **`DescribeImages`** Amazon EC2 pada citra Amazon EC2 yang ingin Anda gunakan untuk membuat citra BYOL.
> - Hubungi Amazon EC2 **`ModifyImageAttribute`** pada citra Amazon EC2 yang ingin Anda gunakan untuk membuat citra BYOL. Pastikan bahwa izin peluncuran pada citra Amazon EC2 tidak dibatasi. Citra harus dibagikan sepanjang proses pembuatan citra BYOL.
>
> Untuk contoh kebijakan IAM khusus untuk BYOL WorkSpaces, lihat. Identitas dan manajemen akses untuk WorkSpaces Untuk informasi lebih lanjut tentang bekerja dengan izin IAM, lihat Mengubah Izin untuk Pengguna IAM dalam Panduan Pengguna IAM. Untuk membuat Graphics.g4dn, GraphicsPro .g4dn, Graphics, atau GraphicsPro bundel dari gambar Anda, hubungi AWS Support Pusat untuk menambahkan akun Anda ke daftar izinkan. Setelah akun Anda berada di daftar izinkan, Anda dapat menggunakan AWS CLI import-workspace-image perintah untuk menelan Graphics.g4dn, .g4dn, Graphics, GraphicsPro atau image. GraphicsPro Untuk informasi selengkapnya, lihat import-workspace-imagedi Referensi AWS CLI Perintah.

Untuk membuat citra dari Windows VM

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Citra.
3. Pilih Buat citra BYOL.
4. Di halaman Buat Citra BYOL, lakukan hal berikut:

   - Untuk ID AMI, pilih tautan Konsol EC2, dan pilih citra Amazon EC2 yang Anda impor seperti yang dijelaskan di bagian sebelumnya (Langkah 5: Impor VM sebagai citra ke Amazon EC2). Nama citra harus dimulai dengan `ami-` dan diikuti oleh pengenal untuk AMI (misalnya, `ami-1234567e`).
   - Untuk Nama citra, masukkan nama yang unik untuk citra.
   - Untuk Deskripsi, masukkan deskripsi untuk membantu Anda mengidentifikasi citra dengan cepat.
   - Untuk jenis Instance, pilih jenis bundel yang sesuai (baik Regular, Graphics.g4dn, Graphics, atau GraphicsPro), tergantung pada protokol yang ingin Anda gunakan untuk gambar Anda, baik PCoIP atau Streaming Protocol (WSP). WorkSpaces Jika Anda ingin membuat GraphicsPro bundel.g4dn, pilih Graphics.g4dn. Untuk bundel yang tidak mendukung GPU (bundel selain Graphics.g4dn, .g4dn, Graphics, atau), pilih Regular. GraphicsPro GraphicsPro

     > **Note**
     >
     > Graphics.g4dn, GraphicsPro .g4dn, Grafik, dan GraphicsPro gambar hanya dapat dibuat untuk protokol PCoIP saat ini.

   - (Opsional) Untuk Pilih aplikasi, pilih versi Microsoft Office yang ingin Anda jadikan langganan. Untuk informasi selengkapnya, lihat Tambahkan Microsoft Office untuk citra BYOL.
   - (Opsional) Untuk Tanda, pilih Tambahkan tanda baru untuk mengaitkan tanda dengan citra ini. Untuk informasi selengkapnya, lihat WorkSpaces Sumber daya tag.
5. Pilih Buat citra BYOL.

   Selagi citra Anda dibuat, status citra pada halaman Citra konsol tersebut muncul sebagai Menunggu. Proses penyerapan BYOL memerlukan waktu minimal 90 menit. Jika Anda juga telah berlangganan ke Office, harap diketahui bahwa proses memakan waktu minimal 3 jam.

   Jika validasi citra tidak berhasil, konsol tersebut menampilkan kode kesalahan. Setelah pembuatan citra selesai, status berubah menjadiTersedia.

Langkah 7: Buat paket kustom dari citra BYOL

Setelah citra BYOL Anda dibuat, Anda dapat menggunakan citra untuk membuat paket kustom. Untuk informasi, lihat Buat WorkSpaces gambar dan bundel khusus.

Langkah 8: Daftarkan direktori khusus untuk WorkSpaces

Untuk menggunakan gambar BYOL WorkSpaces, Anda harus mendaftarkan direktori untuk tujuan ini.

Untuk mendaftarkan direktori untuk WorkSpaces

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih Direktori.
3. Pilih direktori dan pilih Tindakan, Pendaftaran.
4. Dalam kotak dialog Daftar direktori, untuk Aktifkan Khusus WorkSpaces, pilih Ya.
5. PilihPendaftaran.

Jika Anda telah mendaftarkan AWS Managed Microsoft AD direktori atau direktori AD Connector WorkSpaces yang tidak berjalan pada perangkat keras khusus, Anda dapat menyiapkan AWS Managed Microsoft AD direktori baru atau direktori AD Connector untuk tujuan ini. Anda juga dapat membatalkan pendaftaran direktori dan kemudian mendaftarkannya kembali sebagai direktori untuk dedicated. WorkSpaces Untuk melakukannya, lakukan langkah-langkah ini.

> **Note**
>
> Anda hanya dapat melakukan prosedur ini jika tidak WorkSpaces ada yang terkait dengan direktori.

Untuk membatalkan pendaftaran direktori dan mendaftarkannya kembali untuk didedikasikan WorkSpaces

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Mengakhiri yang ada WorkSpaces.
3. Di panel navigasi, pilih Direktori.
4. Pilih direktori dan pilih Tindakan, Batalkan Pendaftaran.
5. Ketika diminta konfirmasi, pilih Batalkan Pendaftaran.

6. Pilih direktori sekali lagi dan pilih Tindakan, Pendaftaran.
7. Dalam kotak dialog Daftar direktori, untuk Aktifkan Khusus WorkSpaces, pilih Ya.
8. PilihPendaftaran.

Langkah 9: Luncurkan BYOL Anda WorkSpaces

Setelah Anda mendaftarkan direktori untuk dedicated WorkSpaces, Anda dapat meluncurkan BYOL Anda WorkSpaces di direktori ini. Untuk informasi tentang cara meluncurkan WorkSpaces, lihatLuncurkan desktop virtual menggunakan WorkSpaces.

Pantau Anda WorkSpaces

Anda dapat menggunakan fitur-fitur berikut untuk memantau Anda WorkSpaces.

CloudWatch metrik

Amazon WorkSpaces menerbitkan poin data ke Amazon CloudWatch tentang Anda WorkSpaces. CloudWatch memungkinkan Anda untuk mengambil statistik tentang titik-titik data tersebut sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anda dapat menggunakan metrik ini untuk memverifikasi kinerja Anda seperti WorkSpaces yang diharapkan. Untuk informasi selengkapnya, lihat Pantau CloudWatch metrik WorkSpaces penggunaan Anda.

CloudWatch Acara

Amazon WorkSpaces dapat mengirimkan acara ke CloudWatch Acara Amazon saat pengguna masuk ke acara Anda WorkSpace. Ini memungkinkan Anda untuk merespons saat peristiwa itu terjadi. Untuk informasi selengkapnya, lihat Pantau Anda WorkSpaces menggunakan Amazon EventBridge.

CloudTrail log

AWS CloudTrail memberikan catatan tindakan yang diambil oleh pengguna, peran, atau layanan AWS di WorkSpaces. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat WorkSpaces, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Mencatat Panggilan WorkSpaces API dengan Menggunakan CloudTrail. AWS CloudTrailmencatat peristiwa login yang berhasil dan tidak berhasil untuk pengguna kartu pintar. Untuk informasi selengkapnya, lihat Memahami peristiwa AWS masuk untuk pengguna kartu pintar.

CloudWatch Monitor Internet

Amazon CloudWatch Internet Monitor memberikan visibilitas tentang bagaimana masalah internet memengaruhi kinerja dan ketersediaan antara aplikasi yang di-host AWS dan pengguna akhir Anda. Anda juga dapat menggunakan CloudWatch Internet Monitor untuk:

- Buat monitor untuk satu atau beberapa WorkSpace direktori.
- Pantau kinerja internet.
- Dapatkan alarm untuk masalah antara jaringan kota pengguna akhir Anda, termasuk lokasinya dan ASN, yang biasanya Penyedia Layanan Internet (ISP), dan Wilayah mereka. WorkSpace

Monitor Internet menggunakan data konektivitas yang AWS dapatkan dari jejak jaringan globalnya untuk menghitung dasar performa dan ketersediaan untuk lalu lintas yang dapat diakses di internet. Internet Monitor saat ini tidak dapat memberikan kinerja internet untuk pengguna akhir individu tetapi dapat di tingkat kota dan ISP.

Pantau WorkSpaces kesehatan Anda menggunakan dasbor CloudWatch otomatis

Anda dapat memantau WorkSpaces menggunakan dasbor CloudWatch otomatis, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Metrik disimpan selama 15 bulan untuk mengakses informasi historis dan untuk memantau kinerja aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

CloudWatch Dasbor dibuat secara otomatis saat Anda menggunakan AWS akun untuk mengonfigurasi akun Anda WorkSpaces. Dasbor memungkinkan Anda memantau WorkSpaces metrik Anda, seperti kesehatan dan kinerjanya, di seluruh Wilayah. Anda juga dapat menggunakan dasbor untuk tujuan berikut:

- Identifikasi WorkSpace contoh yang tidak sehat.
- Identifikasi mode berjalan, protokol, dan sistem operasi yang memiliki instance tidak sehat WorkSpace .
- Lihat pemanfaatan sumber daya penting dari waktu ke waktu.
- Identifikasi anomali untuk membantu pemecahan masalah.

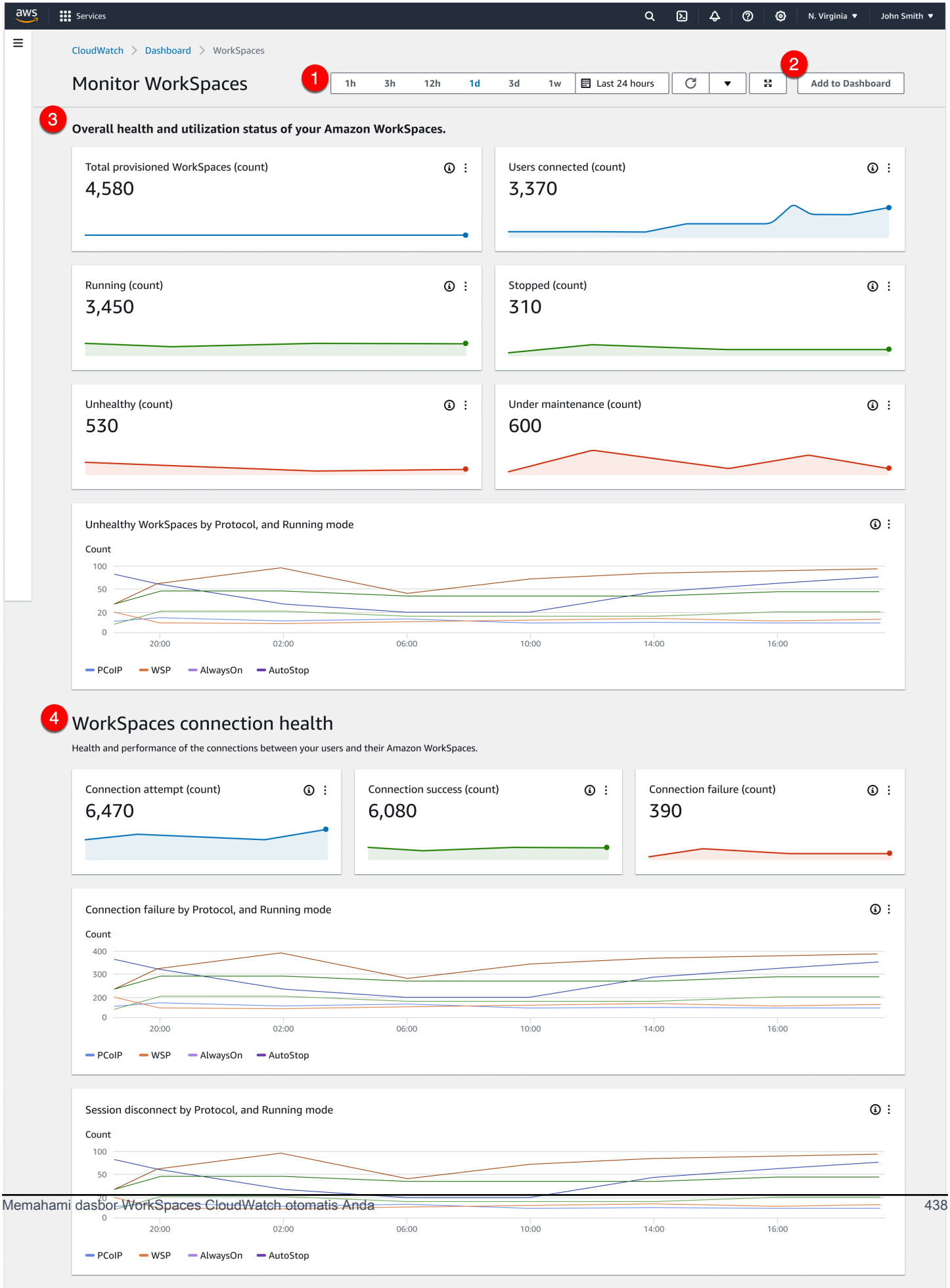
WorkSpaces CloudWatch dasbor otomatis tersedia di semua Wilayah AWS komersial.

Untuk menggunakan dasbor WorkSpaces CloudWatch otomatis

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Dasbor.
3. Pilih tab Dasbor otomatis.
4. Pilih WorkSpaces.

Memahami dasbor WorkSpaces CloudWatch otomatis Anda

Dasbor CloudWatch otomatis memungkinkan Anda untuk mendapatkan wawasan tentang kinerja sumber WorkSpaces daya Anda dan membantu Anda mengidentifikasi masalah kinerja.


aws
Services
N. Virginia
John Smith
CloudWatch > Dashboard > WorkSpaces
Monitor WorkSpaces
1
1h 3h 12h 1d 3d 1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

Dasbor terdiri dari fitur-fitur berikut:

1. Lihat data historis menggunakan kontrol rentang waktu dan tanggal.
2. Tambahkan tampilan dasbor yang disesuaikan ke dasbor CloudWatch khusus.
3. Pantau status kesehatan dan pemanfaatan Anda secara keseluruhan WorkSpaces dengan melakukan hal berikut:
    a. Lihat jumlah total yang disediakan, jumlah pengguna yang terhubung WorkSpaces, jumlah instans yang tidak sehat dan sehat WorkSpace .
    b. Lihat variabel yang tidak sehat WorkSpaces dan variabelnya yang berbeda, seperti protokol dan mode komputasi.
    c. Arahkan kursor ke diagram garis untuk melihat jumlah WorkSpace instans sehat atau tidak sehat untuk protokol tertentu dan mode berjalan selama periode waktu tertentu.
    d. Pilih menu elipsis, lalu pilih Lihat dalam metrik untuk melihat metrik pada bagan skala waktu.
4. Lihat metrik koneksi Anda dan variabelnya yang berbeda, seperti jumlah upaya koneksi, koneksi yang berhasil, dan koneksi yang gagal di WorkSpaces lingkungan Anda pada waktu tertentu.
5. Lihat InSession latensi yang memengaruhi pengalaman pengguna Anda, seperti waktu pulang pergi (RTT), untuk menentukan kesehatan koneksi dan kehilangan paket untuk memantau kesehatan jaringan.
6. Lihat kinerja host dan pemanfaatan sumber daya untuk mengidentifikasi dan memecahkan masalah kinerja potensial.

Pantau CloudWatch metrik WorkSpaces penggunaan Anda

WorkSpaces dan Amazon CloudWatch terintegrasi, sehingga Anda dapat mengumpulkan dan menganalisis metrik kinerja. Anda dapat memantau metrik ini menggunakan CloudWatch konsol, antarmuka baris CloudWatch perintah, atau menggunakan API secara terprogram. CloudWatch CloudWatch juga memungkinkan Anda untuk mengatur alarm ketika Anda mencapai ambang batas tertentu untuk metrik.

Untuk informasi selengkapnya tentang penggunaan CloudWatch dan alarm, lihat Panduan CloudWatch Pengguna Amazon.

Prasyarat

Untuk mendapatkan CloudWatch metrik, aktifkan akses pada port 443 pada `AMAZON` subset di Wilayah. `us-east-1` Untuk informasi selengkapnya, lihat Alamat IP dan persyaratan port untuk WorkSpaces.

Daftar Isi

WorkSpaces metrik

Namespace `AWS/WorkSpaces` mencakup metrik berikut.

Metrik	Deskripsi	Dimensi	Statistik	Unit

`Available` [1]	Jumlah WorkSpaces itu mengembalikan status sehat.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

`Unhealthy` [1]	Jumlah WorkSpaces itu mengembalikan status yang tidak sehat.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

Metrik	Deskripsi	Dimensi	Statistik	Unit

`ConnectionAttempt` [2]	Jumlah upaya hubungan.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

`ConnectionSuccess` [2]	Jumlah hubungan yang berhasil.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

`ConnectionFailure` [2]	Jumlah hubungan yang gagal.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

Metrik	Deskripsi	Dimensi	Statistik	Unit
SessionLaunchTime [2, 6]	Jumlah waktu yang dibutuhkan untuk memulai WorkSpaces sesi.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Kedua (waktu)
InSessionLatency [2, 6]	Waktu pulang pergi antara WorkSpaces klien dan WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Milidetik (waktu)
SessionDisconnect [2, 6]	Jumlah hubungan yang ditutup, termasuk hubungan yang dimulai pengguna dan gagal.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

Metrik	Deskripsi	Dimensi	Statistik	Unit

`UserConnected` [3]	Jumlah WorkSpaces yang memiliki pengguna yang terhubung.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

`Stopped`	Jumlah WorkSpaces itu dihentikan.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

`Maintenance` [4]	Jumlah WorkSpaces yang sedang dalam pemeliharaan.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan

Metrik	Deskripsi	Dimensi	Statistik	Unit
TrustedDeviceValidationAttempt [5, 6]	Jumlah upaya validasi tanda tangan autentikasi perangkat.	DirectoryId	Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan
TrustedDeviceValidationSuccess [5, 6]	Jumlah validasi tanda tangan autentikasi perangkat yang berhasil.	DirectoryId	Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan
TrustedDeviceValidationFailure [5, 6]	Jumlah validasi tanda tangan autentikasi perangkat yang gagal.	DirectoryId	Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan
TrustedDeviceCertificateDaysBeforeExpiration [6]	Hari tersisa sebelum sertifikat root yang terkait dengan direktori kedaluwarsa.	CertificateId	Rata-rata, Jumlah, Maksimum, Minimum, Sampel Data	Hitungan
CPUUsage	Persentase sumber daya CPU yang digunakan.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Rata-rata, Maksimum, Minimum	Persentase

Metrik	Deskripsi	Dimensi	Statistik	Unit
MemoryUsage	Persentase memori mesin yang digunakan.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Rata-rata, Maksimum, Minimum	Persentase
RootVolumeDiskUsage	Persentase volume root disk yang digunakan.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Rata-rata, Maksimum, Minimum	Persentase
UserVolumeDiskUsage	Persentase volume disk pengguna yang digunakan.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Rata-rata, Maksimum, Minimum	Persentase

Metrik	Deskripsi	Dimensi	Statistik	Unit

`UDPPacketLossRate` [7]	Persentase paket turun antara klien dan gateway.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Maksimum, Minimum, Sampel Data	Persentase

`UpTime`	Waktu sejak reboot terakhir dari a WorkSpace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Rata-rata, Maksimum, Minimum, Sampel Data	Detik

[1] WorkSpaces secara berkala mengirimkan permintaan status ke a WorkSpace. A WorkSpace ditandai `Available` ketika menanggapi permintaan ini, dan `Unhealthy` ketika gagal menanggapi permintaan ini. Metrik ini tersedia pada WorkSpace tingkat granularitas per-, dan juga dikumpulkan untuk semua WorkSpaces dalam suatu organisasi.

[2] WorkSpaces mencatat metrik pada koneksi yang dibuat untuk masing-masing WorkSpace. Metrik ini dipancarkan setelah pengguna berhasil diautentikasi melalui WorkSpaces klien dan klien kemudian memulai sesi. Metrik tersedia pada WorkSpace tingkat granularitas per-, dan juga digabungkan untuk semua WorkSpaces dalam direktori.

[3] WorkSpaces secara berkala mengirimkan permintaan status koneksi ke a WorkSpace. Pengguna dilaporkan terhubung saat mereka secara aktif menggunakan sesi. Metrik ini tersedia pada WorkSpace tingkat granularitas per-, dan juga dikumpulkan untuk semua WorkSpaces dalam suatu organisasi.

[4] Metrik ini berlaku untuk WorkSpaces yang dikonfigurasi dengan mode AutoStop berjalan. Jika Anda mengaktifkan pemeliharaan untuk Anda WorkSpaces, metrik ini menangkap jumlah WorkSpaces yang saat ini sedang dalam pemeliharaan. Metrik ini tersedia pada WorkSpace tingkat granularitas per-, yang menjelaskan kapan a WorkSpace masuk ke pemeliharaan dan kapan dihapus.

[5] Jika fitur perangkat tepercaya diaktifkan untuk direktori, Amazon WorkSpaces menggunakan otentikasi berbasis sertifikat untuk menentukan apakah perangkat dipercaya. Saat pengguna mencoba mengaksesnya WorkSpaces, metrik ini dipancarkan untuk menunjukkan otentikasi perangkat tepercaya yang berhasil atau gagal. Metrik ini tersedia pada tingkat perincian per direktori, dan hanya untuk aplikasi klien Amazon Windows WorkSpaces dan macOS.

[6] Tidak tersedia di Akses WorkSpaces Web.

[7] Metrik ini mengukur rata-rata kehilangan paket.

- Di PCoIP: Mengukur kehilangan paket rata-rata di gateway dari klien.
- Di WSP: Mengukur kehilangan paket rata-rata dari klien menuju gateway.

Dimensi untuk WorkSpaces metrik

Untuk memfilter data metrik, gunakan dimensi berikut.

Dimensi	Deskripsi
`DirectoryId`	Memfilter data metrik ke WorkSpaces dalam direktori yang ditentukan. Format ID direktori adalah `d-XXXXXXXXXX` .
`WorkspaceId`	Menyaring data metrik ke yang ditentukan WorkSpace. Bentuk WorkSpace ID adalah`ws-XXXXXXXXXX` .
`CertificateId`	Memfilter data metrik ke sertifikat root tertentu yang terkait dengan direktori. Format ID sertifikat adalah `wsc-XXXXXXXXX` .

Dimensi	Deskripsi
`RunningMode`	Memfilter data metrik ke WorkSpaces mode berjalan mereka. Bentuk mode berjalan adalah AutoStop atau AlwaysOn.
`BundleId`	Memfilter data metrik ke protokol. WorkSpaces Bentuk bundel adalah`wsb-XXXXXXXXXX` .
`ComputeType`	Memfilter data metrik ke WorkSpaces menurut jenis komputasi.

Contoh pemantauan

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan AWS CLI untuk menanggapi CloudWatch alarm dan menentukan mana WorkSpaces dalam direktori yang mengalami kegagalan koneksi.

Untuk menanggapi CloudWatch alarm

1. Tentukan direktori yang digunakan alarm untuk menggunakan perintah jelaskan-alarms.

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. Dapatkan daftar WorkSpaces di direktori yang ditentukan menggunakan perintah deskripsi-ruang kerja.

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. Dapatkan CloudWatch metrik untuk masing-masing WorkSpace di direktori menggunakan get-metric-statisticsperintah.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
```

```
    },
    {
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Pantau Anda WorkSpaces menggunakan Amazon EventBridge

Anda dapat menggunakan acara dari Amazon WorkSpaces untuk melihat, mencari, mengunduh, mengarsipkan, menganalisis, dan menanggapi login yang berhasil ke akun Anda WorkSpaces. Misalnya, Anda dapat menggunakan peristiwa untuk tujuan berikut:

- Simpan atau arsipkan peristiwa WorkSpaces login sebagai log untuk referensi future, analisis log untuk mencari pola, dan mengambil tindakan berdasarkan pola tersebut.
- Gunakan alamat IP WAN untuk menentukan dari mana pengguna masuk, dan kemudian gunakan kebijakan untuk memungkinkan pengguna mengakses hanya ke file atau data WorkSpaces yang memenuhi kriteria akses yang ditemukan dalam jenis acara`WorkSpaces Access`.
- Analisis data login dan lakukan tindakan otomatis menggunakan AWS Lambda.
- Menggunakan kontrol kebijakan untuk memblokir akses ke file dan aplikasi dari alamat IP yang tidak sah.
- Cari tahu versi WorkSpaces klien yang digunakan untuk terhubung WorkSpaces.

Amazon WorkSpaces memancarkan peristiwa ini dengan upaya terbaik. Acara dikirimkan ke EventBridge dalam waktu dekat. Dengan EventBridge, Anda dapat membuat aturan yang memicu tindakan terprogram sebagai respons terhadap suatu peristiwa. Misalnya, Anda dapat mengonfigurasi aturan yang memanggil topik SNS untuk mengirim pemberitahuan email atau memanggil fungsi Lambda untuk mengambil beberapa tindakan. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

WorkSpaces Mengakses acara

WorkSpaces aplikasi klien mengirim `WorkSpaces Access` peristiwa ketika pengguna berhasil masuk ke file WorkSpace. Semua WorkSpaces klien mengirimkan acara ini.

Peristiwa yang dipancarkan untuk WorkSpaces menggunakan Protokol WorkSpaces Streaming (WSP) memerlukan aplikasi WorkSpaces klien versi 4.0.1 atau yang lebih baru.

Peristiwa direpresentasikan sebagai objek JSON. Berikut ini adalah contoh data untuk peristiwa `WorkSpaces Access`.


```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```


Bidang khusus peristiwa

`clientIpAddress`

Alamat IP WAN dari aplikasi client. Untuk client zero PCoIP, alamat ini adalah alamat IP dari client autentikasi Teradici.

`actionType`

Nilai ini selalu `successfulLogin`.

`workspacesClientProductName`

Nilai berikut ini peka terhadap huruf besar-kecil.

- `WorkSpaces Desktop client` — Client Windows, macOS, dan Linux
- `Amazon WorkSpaces Mobile client` — Client iOS

- `WorkSpaces Mobile Client` — Client Android
- `WorkSpaces Chrome Client` — Client Chromebook
- `WorkSpacesWebClient` — Client Akses Web
- `AmazonWorkSpacesThinClient`— Perangkat Amazon WorkSpaces Thin Client
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` — Client Zero

`loginTime`

Waktu di mana pengguna masuk ke WorkSpace.

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

Pengidentifikasi direktori untuk file. WorkSpace Anda harus menambahkan pengidentifikasi direktori dengan `domain/`. Misalnya, `"domain/d-123456789"`.

`clientVersion`

Versi klien yang digunakan untuk terhubung ke WorkSpaces.

`workspaceId`

Pengidentifikasi dari. WorkSpace

Buat aturan untuk menangani WorkSpaces acara

Gunakan prosedur berikut untuk membuat aturan untuk menangani WorkSpaces peristiwa.

Prasyarat

Untuk menerima notifikasi email, buat topik Amazon Simple Notification Service.

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Di panel navigasi, pilih Pengguna.
3. Pilih Buat topik.
4. Untuk Tipe, pilih Standar.
5. Untuk Nama, masukkan nama untuk topik Anda.
6. Pilih Buat topik.
7. Pilih Buat langganan.
8. Untuk Protokol, pilih Email.
9. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima pemberitahuan.
10. Pilih Buat langganan.
11. Anda akan menerima pesan email dengan baris subjek berikut: AWS Notification - Subscription Confirmation. Ikuti petunjuk untuk mengonfirmasi langganan Anda.

Untuk membuat aturan untuk menangani WorkSpaces peristiwa

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Pilih Buat aturan.
3. Untuk Nama, masukkan nama untuk topik Anda.
4. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
5. Pilih Berikutnya.
6. Untuk Pola peristiwa, lakukan hal berikut:
    a. Untuk Sumber peristiwa, pilih Layanan AWS.
    b. Untuk Layanan AWS, pilih WorkSpaces.
    c. Untuk jenis Acara, pilih WorkSpacesAkses.
    d. Secara default, kami mengirim pemberitahuan untuk setiap acara. Jika mau, Anda dapat membuat pola acara yang memfilter acara untuk klien atau ruang kerja tertentu.
7. Pilih Berikutnya.
8. Tentukan target sebagai berikut:

a. Untuk Tipe target, pilih Layanan AWS.

b. Untuk Pilih target, pilih topik SNS.

c. Untuk Topik, pilih topik SNS yang Anda buat untuk notifikasi.

9. Pilih Berikutnya.
10. (Opsional) Tambahkan tanda ke aturan Anda.
11. Pilih Berikutnya.
12. Pilih Buat aturan.

Memahami peristiwa AWS masuk untuk pengguna kartu pintar

AWS CloudTrailmencatat peristiwa login yang berhasil dan tidak berhasil untuk pengguna kartu pintar. Ini termasuk peristiwa login yang ditangkap setiap kali pengguna diminta untuk menyelesaikan tantangan atau faktor kredenal tertentu, serta status permintaan verifikasi kredenal tertentu. Pengguna masuk hanya setelah menyelesaikan semua tantangan kredensi yang diperlukan, yang mengakibatkan `UserAuthentication` peristiwa dicatat.

Tabel berikut menangkap setiap nama CloudTrail acara masuk dan tujuannya.

Nama peristiwa	Tujuan acara
`CredentialChallenge`	Memberitahu bahwa AWS login telah meminta pengguna menyelesaikan tantangan kredenal tertentu dan menentukan `CredentialType` yang diperlukan (misalnya, SMARTCARD).
`CredentialVerification`	Memberitahu bahwa pengguna telah mencoba untuk memecahkan `CredentialChallenge` permintaan tertentu, dan menentukan apakah kredensi tersebut telah berhasil atau gagal.
`UserAuthentication`	Memberitahu bahwa semua persyaratan otentikasi yang ditantang pengguna telah berhasil diselesaikan dan bahwa pengguna berhasil masuk. Ketika pengguna gagal menyelesaikan tantangan kredensi yang diperlukan dengan sukses, tidak ada `UserAuthentication` peristiwa yang dicatat.

Tabel berikut menangkap bidang data peristiwa berguna tambahan yang terdapat dalam peristiwa login CloudTrail tertentu.

Nama peristiwa	Tujuan acara	Penerapan acara masuk	Contoh nilai
`AuthWorkflowID`	Mengkorelasikan semua peristiwa yang dipancarkan di seluruh urutan masuk. Untuk setiap login pengguna, beberapa peristiwa dapat dipancarkan dengan login. AWS	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	“AuthWorkflowID”: “9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	Memberitahu bahwa pengguna telah mencoba untuk memecahkan `CredentialChallenge` permintaan tertentu dan menentukan apakah kredensi tersebut telah berhasil atau gagal.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType“: “SMARTCARD” (nilai yang mungkin hari ini: SMARTCARD)
`LoginTo`	Memberitahu bahwa semua persyaratan otentikasi yang ditantang pengguna telah berhasil diselesaikan dan bahwa pengguna berhasil masuk. Ketika pengguna gagal menyelesaikan tantangan kredensi yang diperlukan dengan sukses, tidak ada `UserAuthentication` peristiwa yang dicatat.	`UserAuthentication`	“LoginTo“:" https://skylight.local”

Contoh peristiwa untuk AWS skenario login

Contoh berikut menunjukkan urutan CloudTrail peristiwa yang diharapkan untuk skenario masuk yang berbeda.

Daftar Isi

Masuk berhasil saat mengautentikasi dengan kartu pintar

Urutan peristiwa berikut menangkap contoh login kartu pintar yang sukses.

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
```

```
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Sukses CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
```

```
        CredentialVerification": "Success"
    }
}
```

Sukses UserAuthentication

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```

Gagal masuk saat mengautentikasi hanya dengan kartu pintar

Urutan peristiwa berikut menangkap contoh login kartu pintar yang gagal.

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Gagal CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

Kelangsungan bisnis untuk Amazon WorkSpaces

Amazon WorkSpaces dibangun di atas infrastruktur AWS global, yang diatur ke dalam AWS Wilayah dan Zona Ketersediaan. Wilayah dan Availability Zones ini memberikan ketahanan dalam hal isolasi fisik dan redundansi data. Untuk informasi selengkapnya, lihat Ketahanan di Amazon WorkSpaces.

Amazon WorkSpaces juga menyediakan pengalihan lintas wilayah, fitur yang berfungsi dengan kebijakan perutean Sistem Nama Domain (DNS) Anda untuk mengarahkan WorkSpaces pengguna Anda ke alternatif WorkSpaces saat primer mereka tidak tersedia. WorkSpaces Misalnya, dengan menggunakan kebijakan perutean failover DNS, Anda dapat menghubungkan pengguna Anda ke WorkSpaces Wilayah failover yang ditentukan ketika mereka tidak dapat mengakses mereka WorkSpaces di Wilayah utama.

Anda dapat menggunakan pengalihan lintas wilayah untuk mencapai ketahanan wilayah dan ketersediaan yang tinggi. Anda juga dapat menggunakannya untuk tujuan lain, seperti distribusi lalu lintas atau memberikan alternatif WorkSpaces selama periode pemeliharaan. Jika Anda menggunakan Amazon Route 53 untuk konfigurasi DNS Anda, Anda dapat memanfaatkan pemeriksaan kesehatan yang memantau CloudWatch alarm Amazon.

Ketahanan WorkSpaces Multi-Wilayah Amazon menyediakan infrastruktur desktop virtual yang otomatis dan berlebihan di WorkSpace Wilayah sekunder dan merampingkan proses pengalihan pengguna ke Wilayah sekunder ketika Wilayah utama tidak dapat dijangkau karena pemadaman.

Anda dapat menggunakan Ketahanan WorkSpaces Multi-Wilayah dengan pengalihan Lintas wilayah untuk menerapkan infrastruktur desktop virtual yang berlebihan di WorkSpace Wilayah sekunder dan merancang strategi failover lintas wilayah sebagai persiapan untuk peristiwa yang mengganggu. Anda juga dapat menggunakan solusi ini untuk tujuan lain, seperti distribusi lalu lintas atau memberikan alternatif WorkSpaces selama periode pemeliharaan. Jika Anda menggunakan Route 53 untuk konfigurasi DNS Anda, Anda dapat memanfaatkan pemeriksaan kesehatan yang memantau CloudWatch alarm.

Konten

Pengalihan Lintas Wilayah untuk Amazon WorkSpaces

Dengan fitur pengalihan lintas wilayah di Amazon WorkSpaces, Anda dapat menggunakan nama domain yang memenuhi syarat (FQDN) sebagai kode pendaftaran untuk Anda. WorkSpaces Pengalihan Lintas Wilayah berfungsi dengan kebijakan perutean Sistem Nama Domain (DNS) Anda untuk mengarahkan WorkSpaces pengguna Anda ke alternatif WorkSpaces saat primer mereka tidak tersedia. WorkSpaces Misalnya, dengan menggunakan kebijakan perutean failover DNS, Anda dapat menghubungkan pengguna Anda ke WorkSpaces Wilayah failover yang ditentukan ketika mereka tidak dapat mengakses mereka WorkSpaces di AWS Wilayah utama.

Anda dapat menggunakan pengalihan lintas wilayah bersama dengan kebijakan perutean failover DNS Anda untuk mencapai ketahanan wilayah dan ketersediaan tinggi. Anda juga dapat menggunakan fitur ini untuk tujuan lain, seperti distribusi lalu lintas atau memberikan alternatif WorkSpaces selama periode pemeliharaan. Jika Anda menggunakan Amazon Route 53 untuk konfigurasi DNS Anda, Anda dapat memanfaatkan pemeriksaan kesehatan yang memantau CloudWatch alarm Amazon.

Untuk menggunakan fitur ini, Anda harus menyiapkan WorkSpaces untuk pengguna Anda di dua (atau lebih) AWS Wilayah. Anda juga harus membuat kode registrasi berbasis FQDN khusus yang disebut Alias hubungan. Alias koneksi ini menggantikan kode pendaftaran khusus Wilayah untuk pengguna Anda. WorkSpaces (Kode pendaftaran khusus wilayah tetap valid; namun, untuk pengalihan lintas wilayah untuk bekerja, pengguna Anda harus menggunakan FQDN sebagai gantinya sebagai kode registrasi mereka.)

Untuk membuat alias hubungan, Anda menentukan string hubungan, yang merupakan FQDN Anda, seperti `www.example.com` atau`desktop.example.com`. Untuk menggunakan domain ini untuk pengalihan lintas wilayah, Anda harus mendaftarkannya dengan pendaftar domain dan mengonfigurasi layanan DNS untuk domain Anda.

Setelah Anda membuat alias koneksi, Anda mengaitkannya dengan WorkSpaces direktori Anda di Wilayah yang berbeda untuk membuat pasangan asosiasi. Setiap pasangan asosiasi memiliki Wilayah utama dan satu Wilayah failover atau lebih. Jika terjadi pemadaman di Wilayah utama, kebijakan perutean failover DNS Anda akan mengarahkan WorkSpaces pengguna Anda ke WorkSpaces yang telah Anda siapkan untuk mereka di Wilayah failover.

Untuk menentukan wilayah utama dan failover, Anda menentukan prioritas Wilayah (primer atau sekunder) ketika mengonfigurasi kebijakan perutean failover DNS.

Daftar Isi

Prasyarat

- Anda harus memiliki dan mendaftarkan domain yang ingin Anda gunakan sebagai FQDN dalam alias hubungan Anda. Jika Anda belum menggunakan pendaftar domain lain, Anda dapat menggunakan Amazon Route 53 untuk mendaftarkan domain Anda. Untuk informasi selengkapnya, lihat Mendaftarkan nama domain dengan Amazon Route 53 dalam Panduan Developer Amazon Route 53.

> **Important**
>
> Anda harus memiliki semua hak yang diperlukan untuk menggunakan nama domain apa pun yang Anda gunakan bersama dengan Amazon WorkSpaces. Anda setuju bahwa nama domain tidak melanggar atau menyalahi hak legal pihak ketiga mana pun atau melanggar hukum yang berlaku.

Panjang total nama domain Anda tidak boleh melebihi 255 karakter. Untuk informasi selengkapnya tentang nama domain, lihat Format nama domain DNS di Panduan Developer Amazon Route 53 Panduan.

Pengalihan lintas wilayah bekerja dengan nama domain publik dan nama domain di zona DNS privat. Jika Anda menggunakan zona DNS pribadi, Anda harus menyediakan koneksi jaringan pribadi virtual (VPN) ke virtual private cloud (VPC) yang berisi Anda. WorkSpaces Jika WorkSpaces pengguna Anda mencoba menggunakan FQDN pribadi dari internet publik, aplikasi WorkSpaces klien mengembalikan pesan galat berikut:

```
"We're unable to register the WorkSpace because of a DNS server issue.
Contact your administrator for help."
```

- Anda harus menyiapkan layanan DNS Anda dan mengonfigurasi kebijakan perutean DNS yang diperlukan. Pengalihan Lintas Wilayah berfungsi bersama dengan kebijakan perutean DNS Anda untuk mengarahkan pengguna sesuai kebutuhan. WorkSpaces
- Di setiap Wilayah primer dan failover tempat Anda ingin mengatur pengalihan lintas wilayah, buat WorkSpaces untuk pengguna Anda. Pastikan Anda menggunakan nama pengguna yang sama di setiap WorkSpaces direktori di setiap Wilayah. Agar data pengguna Active Directory tetap sinkron, sebaiknya gunakan AD Connector untuk menunjuk ke Active Directory yang sama di setiap Wilayah tempat Anda menyiapkan WorkSpaces untuk pengguna. Untuk informasi selengkapnya tentang membuat WorkSpaces, lihat Peluncuran WorkSpaces.

> **Important**
>
> Jika Anda mengonfigurasi direktori Microsoft AD AWS Terkelola untuk replikasi Multi-wilayah, hanya direktori di Wilayah utama yang dapat didaftarkan untuk digunakan dengan Amazon. WorkSpaces Upaya untuk mendaftarkan direktori di Wilayah yang direplikasi untuk digunakan dengan Amazon WorkSpaces akan gagal. Replikasi Multi-Wilayah dengan AWS Microsoft AD Terkelola tidak didukung untuk digunakan dengan Amazon WorkSpaces dalam Wilayah yang direplikasi.

Setelah selesai menyiapkan pengalihan lintas wilayah, Anda harus memastikan WorkSpaces pengguna Anda menggunakan kode registrasi berbasis FQDNN, bukan kode registrasi berbasis Region (misalnya,) untuk Wilayah utama mereka. `WSpdx+ABC12D` Untuk melakukan ini, Anda

harus mengirim email pada pengguna dengan string hubungan FQDN dengan menggunakan prosedur di Langkah 5: Kirim string koneksi ke WorkSpaces pengguna Anda.

> **Note**
>
> Jika Anda membuat pengguna di WorkSpaces konsol alih-alih membuatnya di Active Directory, WorkSpaces secara otomatis mengirimkan email undangan ke pengguna Anda dengan kode registrasi berbasis Wilayah setiap kali Anda meluncurkan yang baru. WorkSpace Ini berarti bahwa ketika Anda mengatur WorkSpaces untuk pengguna Anda di Wilayah failover, pengguna Anda juga akan secara otomatis menerima email untuk failover WorkSpaces ini. Anda perlu menginstruksikan pengguna Anda untuk mengabaikan email dengan kode registrasi berbasis Wilayah.

Batasan

- Pengalihan Lintas Wilayah tidak secara otomatis memeriksa apakah koneksi ke Wilayah utama gagal dan kemudian gagal Anda WorkSpaces ke Wilayah lain. Dengan kata lain, failover otomatis tidak terjadi.

  Untuk menerapkan skenario failover otomatis, Anda harus menggunakan beberapa mekanisme lain dalam hubungannya dengan pengalihan lintas wilayah. Misalnya, Anda dapat menggunakan kebijakan perutean DNS failover Amazon Route 53 yang dipasangkan dengan pemeriksaan kesehatan Route 53 yang memantau CloudWatch alarm di Wilayah utama. Jika CloudWatch alarm di Wilayah utama dipicu, kebijakan perutean failover DNS Anda akan mengarahkan WorkSpaces pengguna ke WorkSpaces yang telah Anda atur untuk mereka di Wilayah failover.
- Saat Anda menggunakan pengalihan Lintas wilayah, data pengguna tidak disimpan WorkSpaces di antara Wilayah yang berbeda. Untuk memastikan bahwa pengguna dapat mengakses file mereka dari Wilayah yang berbeda, kami sarankan Anda menyiapkan Amazon WorkDocs untuk WorkSpaces pengguna Anda, jika Amazon WorkDocs didukung di Wilayah utama dan failover Anda. Untuk informasi selengkapnya tentang Amazon WorkDocs, lihat Amazon WorkDocs Drive di Panduan WorkDocs Administrasi Amazon. Untuk informasi selengkapnya tentang mengaktifkan Amazon WorkDocs untuk WorkSpace pengguna Anda, lihat Daftarkan direktori dengan WorkSpaces danAktifkan Amazon WorkDocs untuk Microsoft AD yang AWS Dikelola. Untuk informasi tentang cara WorkSpaces pengguna dapat mengatur Amazon WorkDocs di Amazon WorkSpaces, lihat Mengintegrasikan dengan WorkDocs di Panduan WorkSpaces Pengguna Amazon.

- Pengalihan Lintas Wilayah hanya didukung pada versi 3.0.9 atau yang lebih baru dari aplikasi klien Linux, macOS, dan Windows. WorkSpaces Anda juga dapat menggunakan pengalihan lintas wilayah dengan Akses Web.
- Pengalihan Lintas Wilayah tersedia di semua AWSWilayah di mana Amazon WorkSpaces tersedia, kecuali untuk AWS GovCloud (US) Region s dan Wilayah China (Ningxia).

Langkah 1: Buat alias hubungan

Menggunakan akun AWS yang sama, buat alias hubungan di setiap Wilayah utama dan failover tempat Anda ingin mengatur pengalihan lintas Wilayah.

Untuk membuat alias

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol, pilih AWS Wilayah utama untuk Anda. WorkSpaces
3. Di panel navigasi, pilih Pengaturan Akun.
4. Di bagian Pengalihan lintas-Wilayah pilih Buat alias hubungan.
5. Untuk String hubungan, masukkan FQDN, seperti `www.example.com`atau `desktop.example.com`. Sebuah hubungan string dapat mencapai 255 karakter maksimal. Hal ini dapat mencakup hanya huruf (A-Z dan a-z), angka (0-9), dan karakter berikut: .-

   > **Important**
   >
   > Setelah Anda membuat string hubungan, string tersebut selalu dikaitkan dengan akun AWS. Anda tidak dapat membuat ulang string hubungan yang sama dengan akun yang berbeda, bahkan jika Anda menghapus semua instans dari akun asli. String hubungan secara global disediakan untuk akun Anda.

6. (Opsional) Di bagian Tanda, tentukan tanda yang ingin Anda kaitkan dengan alias hubungan Anda.
7. Pilih Buat alias hubungan.
8. Ulangi langkah-langkah iniStep 2, tetapi di, pastikan untuk memilih Wilayah failover untuk Anda WorkSpaces. Jika Anda memiliki lebih dari satu Wilayah failover, ulangi langkah berikut untuk setiap Wilayah failover. Pastikan untuk menggunakan akun AWS yang sama untuk membuat alias hubungan di setiap Wilayah failover.

(Opsional) Langkah 2: Bagikan alias hubungan dengan akun lain

Anda dapat berbagi alias hubungan dengan satu akun AWSdan lainnya di Wilayah AWS yang sama. Berbagi alias hubungan dengan akun lain memberikan izin akun tersebut untuk mengaitkan atau memisahkan alias tersebut dengan direktori yang dimiliki oleh akun tersebut hanya di Wilayah yang sama. Hanya akun yang memiliki alias hubungan yang dapat menghapus hubungan.

> **Note**
>
> Sebuah alias hubungan dapat dikaitkan dengan hanya satu direktori per Wilayah AWS. Jika Anda berbagi alias hubungan dengan akun AWS lain, hanya satu akun (akun Anda atau akun bersama) yang dapat mengaitkan alias dengan direktori di Wilayah tersebut.

Berbagi alias hubungan dengan akun AWS

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol tersebut, pilih Wilayah AWS tempat Anda ingin berbagi alias hubungan dengan akun AWS lain.
3. Di panel navigasi, pilih Pengaturan Akun.
4. Di bagian Kaitan pengalihan Lintas Wilayah, pilih string hubungan, lalu pilih Tindakan, Bagikan/batalkan pembagian alias hubungan.

   Anda juga dapat berbagi alias dari halaman detail untuk alias hubungan Anda. Untuk melakukannya, di bagian Akun bersama Pilih,Alias hubungan.
5. Di halaman Bagikan/batalkan pembagian alias hubungan, di bagian Berbagi dengan akun, masukkan ID akun AWS tempat Anda ingin membagikan alias hubungan di Wilayah AWS.
6. Pilih Bagikan.

Langkah 3: Kaitkan alias hubungan dengan direktori di setiap Wilayah

Mengaitkan alias koneksi yang sama dengan WorkSpaces direktori di dua Wilayah atau lebih membuat pasangan asosiasi antara direktori. Setiap pasangan asosiasi memiliki Wilayah utama dan satu Wilayah failover atau lebih.

Misalnya, jika Wilayah utama Anda adalah Wilayah Barat AS (Oregon), Anda dapat memasangkan WorkSpaces direktori Anda di Wilayah Barat AS (Oregon) dengan WorkSpaces direktori di Wilayah

AS Timur (Virginia N.). Jika terjadi pemadaman di Wilayah utama, pengalihan lintas wilayah berfungsi bersama dengan kebijakan perutean failover DNS Anda dan pemeriksaan kesehatan apa pun yang telah Anda lakukan di Wilayah AS Barat (Oregon) untuk mengarahkan pengguna Anda ke yang telah WorkSpaces Anda siapkan untuk mereka di Wilayah AS Timur (Virginia N.). Untuk informasi selengkapnya tentang pengalaman pengalihan lintas wilayah, lihat Yang terjadi selama pengalihan lintas Wilayah.

> **Note**
>
> Jika WorkSpaces pengguna Anda berada pada jarak yang signifikan dari Wilayah failover (misalnya, ribuan mil jauhnya), WorkSpaces pengalaman mereka mungkin kurang responsif daripada biasanya. Untuk memeriksa waktu pulang pergi (RTT) ke berbagai AWS Wilayah dari lokasi Anda, gunakan Pemeriksaan WorkSpaces Kesehatan Koneksi Amazon.

Untuk mengaitkan alias hubungan dengan direktori

Anda dapat mengaitkan alias hubungan hanya dengan satu direktori per Wilayah AWS. Jika Anda telah membagikan alias hubungan dengan akun AWS lain, hanya satu akun (akun Anda atau akun bersama) yang dapat mengaitkan alias dengan direktori di Wilayah tersebut.

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol, pilih AWS Wilayah utama untuk Anda. WorkSpaces
3. Di panel navigasi, pilih Pengaturan Akun.
4. Di bagian Kaitan pengalihan Lintas Wilayah, pilih string hubungan, kemudian pilih Tindakan, Kaitkan/Pisahkan.

   Anda juga dapat mengaitkan alias hubungan dengan direktori dari halaman detail untuk alias hubungan Anda. Untuk melakukannya, di bagian Direktori terkait pilih,Kaitkan direktori.
5. Di halaman Kaitkan/pisahkan, di bagian Kaitkan ke suatu direktori, pilih direktori tempat Anda ingin mengaitkan alias hubungan di Wilayah AWS.

   > **Note**
   >
   > Jika Anda mengonfigurasi direktori Microsoft AD AWS Terkelola untuk replikasi Multi-wilayah, hanya direktori di Wilayah utama yang dapat digunakan dengan Amazon. WorkSpaces Upaya untuk menggunakan direktori di Wilayah yang direplikasi dengan

Amazon WorkSpaces akan gagal. Replikasi Multi-Wilayah dengan AWS Microsoft AD Terkelola tidak didukung untuk digunakan dengan Amazon WorkSpaces dalam Wilayah yang direplikasi.

6. Pilih Kaitkan.
7. Ulangi langkah-langkah iniStep 2, tetapi di, pastikan untuk memilih Wilayah failover untuk Anda WorkSpaces. Jika Anda memiliki lebih dari satu Wilayah failover, ulangi langkah berikut untuk setiap Wilayah failover. Pastikan untuk mengaitkan alias hubungan yang sama dengan direktori di setiap Wilayah failover.

Langkah 4: Konfigurasikan layanan DNS Anda dan atur kebijakan perutean DNS

Setelah membuat alias hubungan dan pasangan asosiasi alias hubungan, Anda dapat mengonfigurasi layanan DNS untuk domain yang digunakan dalam string hubungan. Anda dapat menggunakan penyedia layanan DNS untuk tujuan ini. Jika Anda belum memiliki penyedia layanan DNS pilihan, Anda dapat menggunakan Amazon Route 53. Untuk informasi selengkapnya, lihat Mengonfigurasi Amazon Route 53 sebagai layanan DNS Anda di Panduan Developer Amazon Route 53.

Setelah mengonfigurasi layanan DNS untuk domain Anda, Anda harus mengatur kebijakan perutean DNS yang ingin Anda gunakan untuk pengalihan lintas Wilayah. Misalnya, Anda dapat menggunakan pemeriksaan kesehatan Amazon Route 53 untuk menentukan apakah pengguna Anda dapat terhubung ke mereka WorkSpaces di Wilayah tertentu. Jika pengguna tidak dapat terhubung, Anda dapat menggunakan kebijakan failover DNS untuk merutekan lalu lintas DNS dari satu Wilayah ke Wilayah lainnya.

Untuk informasi tentang pemilihan kebijakan perutean DNS Anda, lihat Memilih Kebijakan Perutean dalam Panduan Developer Amazon Route 53. Untuk informasi selengkapnya tentang pemeriksaan kondisi Amazon Route 53, lihat Cara Amazon Route 53 memeriksa kondisi sumber daya Anda di Panduan Developer Amazon Route 53.

Saat menyiapkan kebijakan perutean DNS, Anda memerlukan pengenal koneksi untuk asosiasi antara alias koneksi dan WorkSpaces direktori di Wilayah utama. Anda juga akan memerlukan pengenal koneksi untuk asosiasi antara alias koneksi dan WorkSpaces direktori di Wilayah atau Wilayah failover Anda.

> **Note**
>
> Pengenal hubungan tidak sama dengan ID alias hubungan. ID alias hubungan dimulai dengan `wsca-`.

Untuk menemukan pengenal hubungan untuk kaitan alias hubungan

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol, pilih AWS Wilayah utama untuk Anda. WorkSpaces
3. Di panel navigasi, pilih Pengaturan Akun.
4. Di bagian Kaitan pengalihan Lintas Wilayah, pilih teks string hubungan (FQDN) untuk melihat halaman detail alias hubungan.
5. Pada halaman detail untuk alias hubungan Anda, di bagian Direktori terkait, buat catatan dari nilai yang ditampilkan untuk Pengidentifikasi hubungan.
6. Ulangi langkah-langkah iniStep 2, tetapi di, pastikan untuk memilih Wilayah failover untuk Anda WorkSpaces. Jika Anda memiliki lebih dari satu Wilayah failover, ulangi langkah berikut untuk menemukan pengidentifikasi hubungan untuk setiap Wilayah failover.

Contoh: Untuk mengatur kebijakan perutean failover DNS menggunakan Route 53

Contoh berikut membuat zona yang di-hosting publik untuk domain Anda. Namun, Anda dapat mengatur zona yang di-hosting publik atau privat. Untuk informasi selengkapnya tentang zona yang di-hosting privat, lihat Bekerja dengan zona yang di-hosting di Panduan Developer Amazon Route 53.

Contoh ini juga menggunakan kebijakan perutean failover. Anda dapat menggunakan tipe kebijakan perutean lain untuk strategi pengalihan lintas Wilayah Anda. Untuk informasi tentang pemilihan kebijakan perutean DNS Anda, lihat Memilih Kebijakan Perutean dalam Panduan Developer Amazon Route 53.

Ketika Anda menyiapkan kebijakan perutean failover di Route 53, pemeriksaan kondisi diperlukan untuk Wilayah utama. Untuk informasi selengkapnya tentang membuat pemeriksaan kondisi di Route 53, lihat Membuat pemeriksaan kondisi Amazon Route 53 dan mengonfigurasi failover DNS dan Membuat, memperbarui, dan menghapus pemeriksaan kondisi di Panduan Developer Amazon Route 53 Panduan

Jika Anda ingin menggunakan CloudWatch alarm Amazon dengan pemeriksaan kesehatan Route 53, Anda juga perlu mengatur CloudWatch alarm untuk memantau sumber daya di Wilayah utama Anda. Untuk informasi selengkapnya CloudWatch, lihat Apa itu Amazon CloudWatch? di Panduan CloudWatch Pengguna Amazon. Untuk informasi selengkapnya tentang cara Route 53 menggunakan CloudWatch alarm dalam pemeriksaan kesehatannya, lihat Bagaimana Route 53 menentukan status pemeriksaan kesehatan yang memantau CloudWatch alarm dan Memantau CloudWatch alarm di Panduan Pengembang Amazon Route 53.

Untuk mengatur kebijakan perutean failover DNS di Route 53, Anda harus terlebih dahulu membuat zona yang di-hosting untuk domain Anda.

1. Buka konsol Route 53 di https://console.aws.amazon.com/route53/.
2. Di panel navigasi, pilih Zona yang di-hosting, lalu pilih Buat zona yang di-hosting.
3. Di halaman Zona yang di-hosting dibuat, masukkan nama domain Anda (seperti `example.com`) di bagian Nama domain.
4. Di bagian Tipe, Pilih Zona yang di-hosting publik.
5. Pilih Buat Zona yang Di-hosting.

Kemudian buat pemeriksaan kondisi untuk Wilayah utama Anda.

1. Buka konsol Route 53 di https://console.aws.amazon.com/route53/.
2. Di panel navigasi, pilih Pemeriksaan Kondisi, lalu pilih Buat pemeriksaan kondisi.
3. Pada halaman Konfigurasi pemeriksaan kondisi, masukkan nama untuk pemeriksaan kondisi Anda.
4. Untuk Apa yang harus dipantau, pilih Endpoint, Status pemeriksaan kesehatan lainnya (cek kesehatan terhitung), atau Status CloudWatch alarm.
5. Tergantung yang telah Anda pilih di langkah sebelumnya, konfigurasikan pemeriksaan kondisi Anda, lalu pilih Selanjutnya.
6. Di halaman Dapatkan pemberitahuan ketika pemeriksaan kondisi gagal, untuk Buat alarm, pilih Ya atau Tidak.
7. Pilih Buat pemeriksaan kondisi.

Setelah membuat pemeriksaan kondisi, Anda dapat membuat catatan failover DNS.

1. Buka konsol Route 53 di https://console.aws.amazon.com/route53/.

2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Di halaman Zona yang di-hosting, pilih nama domain Anda.
4. Pada halaman detail nama domain Anda, pilih Buat catatan.
5. Di halaman Pilih kebijakan perutean, pilih Failover, lalu pilih Selanjutnya.
6. Di halaman Catatan konfigurasi, di bagian Konfigurasi dasar, untuk Nama catatan, masukkan nama subdomain Anda. Misalnya, jika FQDN Anda `desktop.example.com`, masukkan **`desktop`**.

   > **Note**
   >
   > Jika Anda ingin menggunakan domain akar, biarkan Nama catatan kosong. Namun, sebaiknya gunakan subdomain, seperti `desktop` atau`workspaces`, kecuali jika Anda telah menyiapkan domain semata-mata untuk digunakan bersama Anda WorkSpaces.

7. Untuk Tipe catatan, pilih TXT - Digunakan untuk memverifikasi pengirim email dan untuk nilai-nilai khusus aplikasi.
8. Biarkan pengaturan detik TTL dalam keadaan default.
9. Di bagian Catatan failover untuk ditambahkan ke ***`your_domain_name_`***, pilih Tentukan catatan failover.

Kini Anda perlu mengatur catatan failover untuk Wilayah utama dan failover Anda.

Contoh: Untuk mengatur catatan failover untuk Wilayah utama

1. Di kotak dialog Tentukan catatan failover, untuk Lalu lintas nilai/rute ke, pilih Alamat IP atau nilai lain tergantung pada jenis catatan.
2. Sebuah kotak terbuka bagi Anda untuk memasukkan entri teks sampel Anda. Masukkan pengenal hubungan untuk asosiasi alias hubungan untuk Wilayah utama Anda.
3. Untuk Tipe catatanfailover, pilih Utama.
4. Untuk Pemeriksaan kondisi, pilih pemeriksaan kondisi yang telah Anda buat untuk Wilayah utama Anda.
5. Untuk ID catatan, masukkan deskripsi untuk mengidentifikasi catatan ini.
6. Pilih Tentukan catatan failover. Catatan failover baru Anda muncul di bagian Catatan failover untuk ditambahkan ke ***`your_domain_name_`***.

Contoh: Untuk mengatur catatan failover untuk Wilayah failover

1. Di bagian Catatan failover untuk ditambahkan ke ***your_domain_name_***, pilih Tentukan catatan failover.
2. Di kotak dialog Tentukan catatan failover, untuk Lalu lintas nilai/rute ke, pilih Alamat IP atau nilai lain tergantung pada jenis catatan.
3. Sebuah kotak terbuka bagi Anda untuk memasukkan entri teks sampel Anda. Masukkan pengenal hubungan untuk asosiasi alias hubungan untuk Wilayah failover Anda.
4. Untuk Tipe catatan failover, pilih Utama.
5. (Opsional) Untuk Pemeriksaan Kondisi, masukkan pemeriksaan kondisi yang telah Anda buat untuk Wilayah failover Anda.
6. Untuk ID catatan, masukkan deskripsi untuk mengidentifikasi catatan ini.
7. Pilih Tentukan catatan failover. Catatan failover baru Anda muncul di bagian Catatan failover untuk ditambahkan ke ***your_domain_name_***.

Jika pemeriksaan kesehatan yang telah Anda siapkan untuk Wilayah utama gagal, kebijakan perutean failover DNS akan mengarahkan WorkSpaces pengguna ke Wilayah failover Anda. Route 53 terus memantau pemeriksaan kesehatan untuk Wilayah utama Anda, dan ketika pemeriksaan kesehatan untuk Wilayah utama Anda tidak lagi gagal, Route 53 secara otomatis mengalihkan WorkSpaces pengguna Anda kembali ke Wilayah utama mereka WorkSpaces .

Untuk informasi lebih lanjut tentang membuat catatan DNS, lihat Membuat Catatan Menggunakan Konsol Amazon Route 53 di Panduan Developer Amazon Route 53. Untuk informasi selengkapnya tentang konfigurasi catatan DNS TXT, lihat Tipe catatan TXT di Panduan Developer Amazon Route 53.

Langkah 5: Kirim string koneksi ke WorkSpaces pengguna Anda

Untuk memastikan pengguna Anda WorkSpaces akan diarahkan sesuai kebutuhan selama pemadaman, Anda harus mengirim string koneksi (FQDN) ke pengguna Anda. Jika Anda telah mengeluarkan kode pendaftaran berbasis Wilayah (misalnya,`WSpdx+ABC12D`) kepada WorkSpaces pengguna Anda, kode tersebut tetap berlaku. Namun, agar pengalihan lintas wilayah berfungsi, WorkSpaces pengguna Anda harus menggunakan string koneksi sebagai kode registrasi mereka saat mendaftarkan mereka WorkSpaces di aplikasi WorkSpaces klien.

> **Important**
>
> Jika Anda membuat pengguna di WorkSpaces konsol alih-alih membuatnya di Active Directory, WorkSpaces secara otomatis mengirimkan email undangan ke pengguna Anda dengan kode registrasi berbasis Region (misalnya,`WSpdx+ABC12D`) setiap kali Anda meluncurkan yang baru. WorkSpace Bahkan jika Anda telah mengatur pengalihan lintas wilayah, email undangan yang secara otomatis dikirim untuk new WorkSpaces berisi kode registrasi berbasis Region ini, bukan string koneksi Anda.
> Untuk memastikan WorkSpaces pengguna Anda menggunakan string koneksi alih-alih kode registrasi berbasis Region, Anda harus mengirimi mereka email lain dengan string koneksi dengan menggunakan prosedur di bawah ini.

Untuk mengirim string koneksi ke WorkSpaces pengguna Anda

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol, pilih AWS Wilayah utama untuk Anda. WorkSpaces
3. Di panel navigasi, pilih WorkSpaces.
4. Pada WorkSpaceshalaman, gunakan kotak pencarian untuk mencari pengguna yang ingin Anda kirimi undangan, lalu pilih yang sesuai WorkSpace dari hasil pencarian. Anda hanya dapat memilih satu WorkSpace per satu.
5. Pilih Tindakan, Undang Pengguna.
6. Pada WorkSpaces halaman Undang Pengguna ke Mereka, Anda akan melihat template email untuk dikirim ke pengguna Anda.
7. (Opsional) Jika ada lebih dari satu alias koneksi yang terkait dengan WorkSpaces direktori Anda, pilih string koneksi yang Anda ingin pengguna Anda gunakan dari daftar string alias koneksi. Templat email diperbarui untuk menampilkan string yang telah Anda pilih.
8. Salin teks templat email dan tempelkan ke email pengguna menggunakan aplikasi email Anda sendiri. Dalam aplikasi email Anda, Anda dapat mengubah teks sesuai keperluan. Ketika email undangan siap, kirimkan ke pengguna Anda.

Diagram arsitektur Pengalihan Lintas Wilayah

Diagram berikut menjelaskan proses penyebaran pengalihan lintas wilayah.

> **Note**
>
> Pengalihan Lintas Wilayah hanya memfasilitasi failover dan fallback lintas wilayah. Itu tidak memfasilitasi pembuatan dan pemeliharaan WorkSpaces di Wilayah sekunder dan tidak mengizinkan replikasi data Lintas wilayah. WorkSpaces baik di daerah primer dan sekunder harus dikelola secara terpisah.

Memulai pengalihan lintas wilayah

Jika terjadi pemadaman, Anda dapat memperbarui catatan DNS secara manual atau menggunakan kebijakan perutean otomatis berdasarkan pemeriksaan kesehatan, yang menentukan Wilayah failover. Kami merekomendasikan mengikuti mekanisme pemulihan bencana yang diuraikan dalam Membuat Mekanisme Pemulihan Bencana Menggunakan Amazon Route 53.

Yang terjadi selama pengalihan lintas Wilayah

Selama failover Wilayah, WorkSpaces pengguna Anda terputus dari mereka WorkSpaces di Wilayah utama. Ketika mereka mencoba untuk menghubungkan kembali, mereka menerima pesan kesalahan berikut:

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

Pengguna Anda kemudian diminta untuk masuk kembali. Jika mereka menggunakan FQDN sebagai kode registrasi mereka, ketika mereka masuk lagi, kebijakan perutean failover DNS Anda akan mengarahkan mereka ke kode WorkSpaces yang telah Anda siapkan untuk mereka di Wilayah failover.

> **Note**
>
> Dalam beberapa kasus, pengguna mungkin tidak dapat terhubung kembali saat masuk kembali. Jika perilaku ini terjadi, mereka harus menutup dan memulai ulang aplikasi WorkSpaces klien, dan kemudian mencoba masuk lagi.

Pisahkan alias hubungan dari direktori

Hanya akun yang memiliki direktori dapat memisahkan alias hubungan dari direktori.

Jika Anda telah berbagi alias hubungan dengan akun lain dan akun tersebut telah mengaitkan alias hubungan dengan direktori yang dimiliki oleh akun tersebut, akun tersebut harus digunakan untuk memisahkan alias hubungan dari direktori.

Untuk memisahkan alias hubungan dari direktori

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol tersebut, pilih Wilayah AWS yang berisi alias hubungan yang ingin Anda pisahkan.
3. Di panel navigasi, pilih Pengaturan Akun.
4. Di bagian Kaitan pengalihan lintas Wilayah, pilih string hubungan, kemudian pilih Tindakan, Kaitkan/pisahkan.

   Anda juga dapat memutuskan alias hubungan dari halaman detail alias hubungan. Untuk melakukannya, di bagian Direktori terkait, pilih Batalkan kaitan.
5. Di halaman Kaitkan/pisahkan, pilih Pisahkan.
6. Dalam kotak dialog yang meminta Anda mengonfirmasi pemisahan, pilih Pisahkan.

Batalkan pembagian alias hubungan

Hanya pemilik alias hubungan yang dapat membatalkan alias. Jika Anda membatalkan alias hubungan dengan akun, akun tersebut tidak lagi dapat mengaitkan alias hubungan dengan direktori.

Untuk membatalkan pembagian alias hubungan

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol tersebut, pilih kotak centang Wilayah AWS yang berisi alias hubungan yang ingin Anda hapus.
3. Di panel navigasi, pilih Pengaturan Akun.
4. Di bagian Kaitan pengalihan Lintas Wilayah, pilih string hubungan, lalu pilih Tindakan, Bagikan/batalkan pembagian alias hubungan.

   Anda juga dapat membatalkan pembagian alias hubungan dari halaman detail alias hubungan. Untuk melakukannya, di bagian Akun bersama, pilih Batalkan pembagian.
5. Di halaman Bagikan/batal membagikan alias hubungan, pilih Batalkan pembagian.

6. Dalam kotak dialog yang meminta Anda mengonfirmasi pembatalan pembagian alias hubungan, pilih Batalkan pembagian.

Hapus alias hubungan

Anda dapat menghapus alias hubungan hanya jika itu dimiliki oleh akun Anda dan jika tidak terkait dengan direktori.

Jika Anda telah berbagi alias hubungan dengan akun lain dan akun tersebut telah mengaitkan alias hubungan dengan direktori yang dimiliki oleh akun tersebut, akun tersebut harus memisahkan alias hubungan dari direktori sebelum Anda dapat menghapus alias hubungan.

> **Important**
>
> Setelah Anda membuat string hubungan, string tersebut selalu dikaitkan dengan akun AWS. Anda tidak dapat membuat ulang string hubungan yang sama dengan akun yang berbeda, bahkan jika Anda menghapus semua instans dari akun asli. String hubungan secara global disediakan untuk akun Anda.

> **Warning**
>
> Jika Anda tidak lagi menggunakan FQDN sebagai kode registrasi untuk WorkSpaces pengguna Anda, Anda harus mengambil tindakan pencegahan tertentu untuk mencegah potensi masalah keamanan. Untuk informasi selengkapnya, lihat Pertimbangan keamanan jika Anda berhenti menggunakan pengalihan Lintas Wilayah.

Untuk menghapus alias hubungan

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol tersebut, pilih Wilayah AWS yang berisi alias hubungan yang ingin Anda hapus.
3. Di panel navigasi, pilih Pengaturan Akun.
4. Di bagian Kaitan pengalihan Lintas Wilayah, pilih string hubungan, kemudian pilih Hapus.

   Anda juga dapat menghapus alias hubungan dari halaman detail alias hubungan. Untuk melakukannya, pilih Hapus di sudut kanan atas halaman.

> **Note**
>
> Jika tombol Hapus dinonaktifkan, pastikan bahwa Anda adalah pemilik alias, dan pastikan alias tersebut tidak terkait dengan direktori.

5. Dalam kotak dialog yang meminta Anda mengonfirmasi penghapusan, pilih Hapus.

Izin IAM untuk mengaitkan dan memisahkan alias hubungan

Jika Anda menggunakan pengguna IAM untuk mengaitkan atau memisahkan alias hubungan, pengguna harus memiliki izin untuk `workspaces:AssociateConnectionAlias` dan `workspaces:DisassociateConnectionAlias`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

> **Important**
>
> Jika Anda membuat kebijakan IAM untuk mengaitkan atau membatalkan kaitan alias untuk akun yang tidak memiliki alias hubungan, Anda tidak dapat menentukan ID akun di ARN. Sebaliknya, Anda harus menggunakan * untuk ID akun, seperti yang ditunjukkan dalam kebijakan contoh berikut.
>
> ```
> {
>   "Version": "2012-10-17",
>   "Statement": [
> ```

```
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

Anda dapat menentukan ID akun di ARN hanya jika akun tersebut memiliki alias hubungan untuk dikaitkan atau dipisahkan.

Untuk informasi lebih lanjut tentang bekerja dengan pengguna IAM, lihat Identitas dan manajemen akses untuk WorkSpaces.

Pertimbangan keamanan jika Anda berhenti menggunakan pengalihan Lintas Wilayah

Jika Anda tidak lagi menggunakan FQDN sebagai kode registrasi untuk WorkSpaces pengguna Anda, Anda harus mengambil tindakan pencegahan berikut untuk mencegah potensi masalah keamanan:

- Pastikan untuk mengeluarkan kode registrasi khusus Wilayah kepada WorkSpaces pengguna Anda (misalnya,`WSpdx+ABC12D`) untuk WorkSpaces direktori mereka dan menginstruksikan mereka untuk berhenti menggunakan FQDN sebagai kode registrasi mereka.
- Jika Anda masih memiliki domain ini, pastikan untuk memperbarui catatan DNS TXT Anda untuk menghapus domain ini sehingga tidak dapat dieksploitasi dalam serangan phishing. Jika Anda menghapus domain ini dari catatan DNS TXT Anda dan WorkSpaces pengguna Anda mencoba menggunakan FQDN sebagai kode registrasi mereka, upaya koneksi mereka akan gagal tanpa bahaya.
- Jika Anda tidak lagi memiliki domain ini, WorkSpaces pengguna Anda harus menggunakan kode pendaftaran khusus Wilayah mereka. Jika pengguna terus mencoba menggunakan FQDN sebagai kode pendaftaran mereka, upaya hubungan mereka dapat diarahkan ke situs berbahaya.

Ketahanan Multi-Wilayah untuk Amazon WorkSpaces

Amazon WorkSpaces Multi-Region Resilience (MRR) memungkinkan Anda mengarahkan pengguna ke Wilayah sekunder ketika WorkSpaces Wilayah utama Anda tidak dapat dijangkau karena peristiwa yang mengganggu, tanpa mengharuskan pengguna untuk mengganti kode pendaftaran saat masuk ke siaga mereka. WorkSpaces Standby WorkSpaces adalah fitur Amazon WorkSpaces Multi-Region Resilience yang merampingkan pembuatan dan pengelolaan penerapan siaga. Setelah menyiapkan direktori pengguna di Wilayah sekunder Anda, pilih WorkSpace di Wilayah utama yang ingin Anda buat siaga WorkSpace . Sistem secara otomatis mencerminkan gambar WorkSpace bundel utama ke Wilayah sekunder. Kemudian secara otomatis menyediakan siaga baru WorkSpace di Wilayah sekunder Anda

Ketahanan WorkSpaces Multi-Wilayah Amazon dibangun di atas pengalihan lintas wilayah yang memanfaatkan pemeriksaan kesehatan DNS dan kemampuan failover. Ini memungkinkan Anda untuk menggunakan nama domain yang sepenuhnya memenuhi syarat (FQDN) sebagai kode pendaftaran Anda WorkSpaces . Saat pengguna masuk WorkSpaces, Anda dapat mengarahkan mereka ke seluruh WorkSpaces Wilayah yang didukung berdasarkan kebijakan Sistem Nama Domain (DNS) Anda untuk FQDN. Jika Anda menggunakan Amazon Route 53, sebaiknya gunakan pemeriksaan kesehatan yang memantau CloudWatch alarm Amazon saat merancang strategi pengalihan lintas wilayah. WorkSpaces Untuk informasi selengkapnya, lihat Membuat pemeriksaan kesehatan Amazon Route 53 dan mengonfigurasi failover DNS di Panduan Pengembang Amazon Route 53.

Replikasi data adalah fitur tambahan siaga WorkSpaces yang mereplikasi data satu arah dari Wilayah primer ke Wilayah sekunder. Setelah mengaktifkan replikasi data, snapshot EBS dari sistem dan volume pengguna diambil setiap 12 jam. Ketahanan Multi-Wilayah secara teratur memeriksa snapshot baru. Ketika snapshot ditemukan, ia memulai salinan ke Wilayah sekunder. Saat salinan tiba di Wilayah sekunder, mereka digunakan untuk memperbarui salinan sekunder WorkSpace.

Daftar Isi

- Replikasi data satu arah untuk siaga WorkSpaces

Prasyarat

- Anda harus membuat WorkSpaces untuk pengguna Anda di Wilayah utama sebelum membuat standby WorkSpaces. Untuk informasi selengkapnya tentang membuat WorkSpaces, lihatLuncurkan desktop virtual menggunakan WorkSpaces.
- Untuk mengaktifkan replikasi data saat siaga WorkSpaces, Anda harus memiliki Active Directory yang dikelola sendiri atau AWS Microsoft AD Terkelola yang dikonfigurasi untuk mereplikasi ke Wilayah siaga Anda. Untuk informasi selengkapnya, lihat Membuat direktori Microsoft AD yang AWS Dikelola dan Menambahkan Wilayah yang direplikasi.
- Pastikan Anda memperbarui driver ketergantungan jaringan seperti driver ENA, NVMe, dan PV di primer Anda. WorkSpaces Anda harus melakukan ini setidaknya sekali setiap 6 bulan. Untuk informasi selengkapnya, lihat Menginstal atau memutakhirkan driver Elastic Network Adapter (ENA), Driver AWS NVMeuntuk instance Windows, dan Upgrade driver PV pada instans Windows.
- Pastikan Anda memperbarui agen EC2config, EC2launch, dan EC2launch V2 ke versi terbaru secara berkala. Anda harus melakukan ini setidaknya sekali setiap 6 bulan. Untuk informasi selengkapnya, lihat Memperbarui EC2config dan EC2launch.
- Untuk memastikan replikasi data yang tepat, pastikan Direktori Aktif di wilayah primer dan sekunder disinkronkan untuk FQDN, OU, dan SID pengguna.
- Kuota default (limit) untuk standby WorkSpaces adalah 0. Anda perlu meminta peningkatan kuota layanan sebelum membuat standby WorkSpace. Untuk informasi selengkapnya, lihat WorkSpaces Kuota Amazon.
- Pastikan Anda menggunakan kunci yang dikelola pelanggan untuk mengenkripsi primer dan siaga WorkSpaces Anda. Anda dapat menggunakan kunci Wilayah tunggal atau kunci Multi-wilayah untuk mengenkripsi primer dan siaga Anda. WorkSpaces

Batasan

- Siaga WorkSpaces hanya menyalin gambar bundel primer Anda WorkSpaces tetapi tidak menyalin volume sistem (drive C) atau volume pengguna (drive D) dari primer WorkSpaces Anda. Untuk menyalin volume sistem (drive C) atau volume pengguna (drive D) dari primer WorkSpaces ke standby WorkSpaces, Anda harus mengaktifkan replikasi data.

- Anda tidak dapat langsung memodifikasi, membangun kembali, memulihkan, atau memigrasikan siaga. WorkSpace
- Failover untuk pengalihan lintas wilayah dikendalikan oleh pengaturan DNS Anda. Untuk menerapkan skenario failover otomatis, Anda harus menggunakan mekanisme yang berbeda dalam hubungannya dengan pengalihan lintas wilayah. Misalnya, Anda dapat menggunakan kebijakan perutean DNS failover Amazon Route 53 yang dipasangkan dengan pemeriksaan kesehatan Route 53 yang memantau CloudWatch alarm di Wilayah utama. Jika CloudWatch alarm di Wilayah utama dipanggil, kebijakan perutean failover DNS Anda akan mengarahkan WorkSpaces pengguna ke yang telah Anda atur untuk WorkSpaces mereka di Wilayah failover.
- Replikasi data hanya berjalan satu arah, menyalin data dari Wilayah primer ke Wilayah sekunder. Selama WorkSpaces failover siaga, Anda dapat mengakses data dan aplikasi antara 12 dan 24 jam. Setelah pemadaman, buat cadangan data apa pun yang Anda buat secara manual di sekunder WorkSpace dan keluar. Sebaiknya simpan pekerjaan Anda ke drive eksternal, seperti drive jaringan Anda, sehingga Anda dapat mengakses data Anda dari yang utama WorkSpace.
- Replikasi data tidak mendukung AWS Simple AD.
- Saat Anda mengaktifkan replikasi data saat siaga WorkSpaces, snapshot EBS dari primer WorkSpaces (baik volume root dan sistem) diambil setiap 12 jam. Snapshot awal untuk volume data tertentu penuh dan snapshot berikutnya bersifat inkremental. Akibatnya, replikasi pertama untuk yang diberikan WorkSpace akan memakan waktu lebih lama dari yang berikutnya. Snapshot dimulai pada jadwal yang internal WorkSpaces dan Anda tidak dapat mengontrol waktunya.
- Jika primer WorkSpace dan siaga WorkSpace bergabung menggunakan domain yang sama, kami sarankan Anda hanya terhubung ke primer WorkSpace atau siaga WorkSpace pada titik waktu tertentu untuk menghindari kehilangan koneksi dengan pengontrol domain.
- Jika Anda AWS Managed Microsoft AD mengonfigurasi replikasi Multi-Region, hanya direktori di Wilayah utama yang dapat didaftarkan untuk digunakan. WorkSpaces Jika Anda mencoba mendaftarkan direktori di Wilayah yang direplikasi untuk digunakan WorkSpaces, itu akan gagal. Replikasi Multi-Wilayah dengan AWS Managed Microsoft AD tidak didukung untuk digunakan dengan WorkSpaces dalam Wilayah yang direplikasi.
- Jika Anda telah mengatur pengalihan Lintas wilayah dan membuat WorkSpaces di Wilayah primer dan sekunder tanpa menggunakan standby WorkSpaces, Anda tidak dapat mengonversi yang ada WorkSpace di Wilayah sekunder menjadi siaga secara langsung. WorkSpace Sebagai gantinya, Anda perlu mematikan WorkSpace di Wilayah sekunder Anda, pilih WorkSpace di Wilayah utama yang ingin Anda buat siaga, dan gunakan siaga WorkSpace WorkSpaces untuk membuat siaga. WorkSpace

- Setelah pemadaman, buat cadangan data apa pun yang Anda buat secara manual di sekunder WorkSpace dan keluar. Sebaiknya simpan pekerjaan Anda ke drive eksternal, seperti drive jaringan Anda, sehingga Anda dapat mengakses data Anda dari yang utama WorkSpace.
- WorkSpaces Ketahanan Multi-Wilayah saat ini tersedia di Wilayah berikut:
  - Wilayah AS Timur (Virginia Utara)
  - Wilayah AS Barat (Oregon)
  - Wilayah Eropa (Frankfurt)
  - Wilayah Eropa (Irlandia)
- WorkSpaces Ketahanan Multi-Wilayah hanya didukung pada aplikasi klien Linux, macOS, dan Windows versi 3.0.9 atau yang lebih baru. WorkSpaces Anda juga dapat menggunakan Ketahanan Multi-Wilayah dengan Akses Web.
- WorkSpaces Ketahanan Multi-Wilayah mendukung Windows dan Bring Your Own License (BYOL). WorkSpaces Itu tidak mendukung Amazon Linux, Ubuntu, atau GPU-enabled WorkSpaces (misalnya Graphics WorkSpaces,, Graphics.g4dn GraphicsPro, atau.g4dn). GraphicsPro
- Setelah failover atau failback selesai, tunggu 15 hingga 30 menit sebelum menghubungkan ke file Anda. WorkSpace

Konfigurasikan siaga Ketahanan Multi-Wilayah Anda WorkSpace

Untuk mengonfigurasi siaga Ketahanan Multi-Wilayah Anda WorkSpace

1. Siapkan direktori pengguna di Wilayah primer dan sekunder Anda. Pastikan Anda menggunakan nama pengguna yang sama di setiap WorkSpaces direktori di setiap Wilayah.

   Agar data pengguna Active Directory tetap sinkron, sebaiknya gunakan AD Connector untuk menunjuk ke Active Directory yang sama di setiap Wilayah tempat Anda menyiapkan WorkSpaces untuk pengguna. Untuk informasi selengkapnya tentang membuat direktori, lihat Mendaftarkan direktori dengan WorkSpaces.

   > **Important**
   >
   > Jika Anda mengonfigurasi AWS Managed Microsoft AD direktori untuk replikasi Multi-wilayah, hanya direktori di Wilayah utama yang dapat didaftarkan untuk digunakan. WorkSpaces Upaya untuk mendaftarkan direktori di Wilayah yang direplikasi untuk digunakan WorkSpaces akan gagal. Replikasi Multi-Wilayah dengan AWS Managed

Microsoft AD tidak didukung untuk digunakan dengan WorkSpaces dalam Wilayah yang direplikasi.

2. Buat WorkSpaces untuk pengguna Anda di Wilayah utama. Untuk informasi selengkapnya tentang membuat WorkSpaces, lihat Peluncuran WorkSpaces.
3. Buat siaga WorkSpace di Wilayah sekunder. Untuk informasi selengkapnya tentang membuat siaga WorkSpace, lihat Membuat siaga WorkSpace.
4. Buat dan kaitkan string koneksi (FQDN) dengan direktori pengguna di Wilayah primer dan sekunder.

   Anda harus mengaktifkan pengalihan lintas wilayah di akun Anda karena siaga dibangun berdasarkan WorkSpaces pengalihan lintas wilayah. Ikuti langkah 1 - 3 petunjuk untuk pengalihan Lintas Wilayah untuk Amazon. WorkSpaces
5. Konfigurasikan layanan DNS dan atur kebijakan perutean DNS.

   Anda harus mengatur layanan DNS Anda dan mengonfigurasi kebijakan perutean DNS yang diperlukan. Pengalihan Lintas Wilayah berfungsi bersama dengan kebijakan perutean DNS Anda untuk mengarahkan pengguna sesuai kebutuhan. WorkSpaces
6. Setelah selesai mengatur pengalihan lintas wilayah, Anda harus mengirim email kepada pengguna Anda dengan string koneksi FQDN. Untuk informasi selengkapnya lihat Langkah 5: Kirim string koneksi ke WorkSpaces pengguna Anda. Pastikan WorkSpaces pengguna Anda menggunakan kode registrasi berbasis FQDNN alih-alih kode registrasi berbasis Wilayah (misalnya, WSPDX+ABC12d) untuk Wilayah utama mereka.

   ⚠ Important

   - Jika Anda membuat pengguna di WorkSpaces konsol alih-alih membuatnya di Active Directory, WorkSpaces secara otomatis mengirimkan email undangan ke pengguna Anda dengan kode registrasi berbasis Wilayah setiap kali Anda meluncurkan yang baru. WorkSpace Ini berarti bahwa ketika Anda mengatur WorkSpaces untuk pengguna Anda di Wilayah sekunder, pengguna Anda juga akan secara otomatis menerima email untuk sekunder ini WorkSpaces. Anda perlu menginstruksikan pengguna Anda untuk mengabaikan email dengan kode registrasi berbasis Wilayah.

- Kode pendaftaran khusus Wilayah tetap valid; namun, agar pengalihan lintas Wilayah berfungsi, pengguna Anda harus menggunakan FQDN sebagai gantinya sebagai kode registrasi mereka.

Buat siaga WorkSpace

Sebelum Anda membuat standby WorkSpace, pastikan Anda telah menyelesaikan prasyarat, termasuk membuat direktori pengguna di Wilayah primer dan sekunder, penyediaan WorkSpaces untuk pengguna di Wilayah utama Anda, mengonfigurasi pengalihan lintas wilayah di akun Anda, dan meminta peningkatan batas siaga melalui kuota layanan. WorkSpaces

Untuk membuat siaga WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol, pilih AWS Wilayah utama untuk Anda. WorkSpaces
3. Di panel navigasi, pilih WorkSpaces.
4. Pilih yang ingin WorkSpace Anda buat siaga WorkSpace .
5. Pilih Tindakan dan kemudian pilih Buat siaga WorkSpace.
6. Pilih Region sekunder, di mana Anda akan membuat standby Anda WorkSpace, dan kemudian pilih Berikutnya.
7. Pilih direktori pengguna di Wilayah sekunder Anda dan kemudian pilih Berikutnya.
8. (Opsional) Tambahkan kunci enkripsi, aktifkan enkripsi data, dan kelola tag.

   - Untuk menambahkan kunci enkripsi, masukkan di bawah kunci enkripsi input.
   - Untuk mengaktifkan replikasi data, pilih Aktifkan replikasi data. Kemudian, centang kotak centang untuk mengonfirmasi bahwa Anda mengizinkan biaya bulanan tambahan.
   - Untuk menambahkan tag baru, pilih Tambahkan tag baru.

   Lalu, pilih Selanjutnya.

   > **Note**
   >
   > - Jika aslinya WorkSpace dienkripsi, bidang ini sudah diisi sebelumnya. Namun, Anda dapat memilih untuk menggantinya dengan kunci enkripsi Anda sendiri.

- Dibutuhkan beberapa menit untuk memperbarui status replikasi data.
- Setelah siaga berhasil WorkSpace diperbarui dengan snapshot dari primer WorkSpace, Anda dapat menemukan stempel waktu dari pshot sna di bawah Snapshot Pemulihan.

9. Tinjau pengaturan siaga Anda WorkSpaces dan kemudian pilih Buat.

> **Note**
>
> - Untuk melihat informasi tentang siaga Anda WorkSpaces, buka halaman WorkSpace detail utama.
> - Siaga WorkSpace hanya menyalin gambar bundel primer Anda WorkSpace tetapi tidak menyalin volume sistem (drive C) atau volume pengguna (drive D) dari primer WorkSpaces Anda. Secara default, replikasi data tidak aktif. Untuk menyalin volume sistem (drive C) atau volume pengguna (drive D) dari primer WorkSpaces ke standby WorkSpaces, Anda harus mengaktifkan replikasi data.

Kelola siaga WorkSpace

Anda tidak dapat langsung memodifikasi, membangun kembali, memulihkan, atau memigrasikan siaga. WorkSpace

Untuk mengaktifkan replikasi data untuk siaga Anda WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Pergi ke Wilayah utama Anda, pilih WorkSpace ID utama.
3. Gulir ke bawah ke WorkSpace bagian Standby dan pilih Edit Standby WorkSpace.
4. Pilih Aktifkan replikasi data. Kemudian, centang kotak centang untuk mengonfirmasi bahwa Anda mengizinkan biaya bulanan tambahan. Lalu, pilih Simpan.

> **Note**
>
> - Siaga WorkSpaces tidak bisa hibernasi. Jika Anda menghentikan siaga WorkSpace, itu tidak mempertahankan pekerjaan Anda yang belum diselamatkan. Kami menyarankan

pengguna untuk selalu menyimpan pekerjaan mereka sebelum keluar dari siaga WorkSpaces mereka.

- Untuk mengaktifkan replikasi data saat siaga WorkSpaces, Anda harus memiliki Active Directory yang dikelola sendiri atau AWS Microsoft AD Terkelola yang dikonfigurasi untuk mereplikasi ke Wilayah siaga Anda. Untuk menyiapkan direktori Anda, ikuti langkah 1 hingga 3 di bagian Panduan Membangun kelangsungan bisnis dengan WorkSpaces Amazon AWS dan Layanan Direktori atau lihat Menggunakan Direktori Aktif Terkelola AWS Multi-wilayah dengan Amazon. WorkSpaces Replikasi Multi-Region hanya didukung untuk Edisi Perusahaan AWS Microsoft AD yang Dikelola.
- Dibutuhkan beberapa menit untuk memperbarui status replikasi data.
- Setelah siaga berhasil WorkSpace diperbarui dengan snapshot dari primer WorkSpace, Anda dapat menemukan stempel waktu dari snapshot di bawah Snapshot Pemulihan.

Hapus siaga WorkSpace

Anda dapat mengakhiri siaga dengan cara WorkSpace yang sama Anda mengakhiri reguler. WorkSpace

Untuk menghapus siaga WorkSpace

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di sudut kanan atas konsol, pilih AWS Wilayah utama untuk Anda. WorkSpaces
3. Di panel navigasi, pilih WorkSpaces.
4. Pilih standby WorkSpace dan pilih Delete. Dibutuhkan sekitar 5 menit untuk menghapus siaga WorkSpace. Selama penghapusan, status siaga WorkSpace akan diatur ke Terminating. Ketika penghapusan selesai, siaga WorkSpace menghilang dari konsol.

> **Note**
>
> Menghapus siaga WorkSpace adalah tindakan permanen dan tidak dapat dibatalkan. Data WorkSpace pengguna siaga tidak bertahan dan dihancurkan. Untuk bantuan dengan mencadangkan data pengguna, hubungi AWS Support.

Replikasi data satu arah untuk siaga WorkSpaces

Mengaktifkan replikasi data dalam Ketahanan Multi-Wilayah memungkinkan Anda mereplikasi data dari Wilayah primer ke Wilayah sekunder. Selama kondisi tunak, Ketahanan Multi-Wilayah menangkap snapshot sistem (drive C) dan data (drive D) primer setiap 12 jam. WorkSpaces Snapshot ini ditransfer ke Wilayah sekunder dan digunakan untuk memperbarui siaga WorkSpaces. Secara default, replikasi data dinonaktifkan untuk siaga WorkSpaces.

Setelah replikasi data diaktifkan untuk siaga WorkSpaces, snapshot awal untuk volume data tertentu selesai, sementara snapshot berikutnya bersifat inkremental. Akibatnya, replikasi pertama untuk yang diberikan WorkSpace akan memakan waktu lebih lama dari yang berikutnya. Snapshot dipicu pada interval yang telah ditentukan di dalam WorkSpaces dan waktunya tidak dapat dikontrol oleh pengguna.

Selama failover, ketika pengguna diarahkan ke Wilayah sekunder, mereka dapat mengakses siaga mereka WorkSpaces dengan data dan aplikasi yang berusia antara 12 dan 24 jam. Saat pengguna menggunakan siaga WorkSpaces, Ketahanan Multi-Wilayah tidak akan memaksa mereka untuk keluar dari siaga WorkSpaces atau memperbarui siaga WorkSpaces dengan snapshot dari Wilayah utama.

Setelah pemadaman, pengguna harus secara manual mencadangkan data apa pun yang telah mereka buat di sekunder mereka WorkSpaces sebelum keluar dari siaga WorkSpaces mereka. Ketika mereka masuk lagi, mereka akan diarahkan ke Wilayah utama dan yang utama WorkSpaces.

Keamanan di Amazon WorkSpaces

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

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

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan-layanan AWS di dalam AWS Cloud. AWS juga memberikan Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga melakukan pengujian dan verifikasi secara berkala terhadap efektivitas keamanan kami sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku WorkSpaces, lihat AWSLayanan dalam Lingkup oleh AWS Layanan Program Kepatuhan .
- Keamanan dalam cloud – Tanggung jawab Anda ditentukan oleh layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, mencakup kepekaan data Anda, persyaratan perusahaan, serta peraturan perundangan yang berlaku

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

Konten

Perlindungan data di Amazon WorkSpaces

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

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

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya AWS. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pengelogan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama semua kontrol keamanan bawaan dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan WorkSpaces atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Untuk informasi selengkapnya tentang WorkSpaces dan enkripsi titik akhir FIPS, lihat. Siapkan Amazon WorkSpaces untuk otorisasi FedRAMP atau kepatuhan DoD SRG

Enkripsi diam

Anda dapat mengenkripsi volume penyimpanan untuk WorkSpaces menggunakan AWS KMS Key fromAWS Key Management Service. Untuk informasi selengkapnya, lihat Terenkripsi WorkSpaces.

Saat Anda membuat WorkSpaces dengan volume terenkripsi, gunakan WorkSpaces Amazon Elastic Block Store (Amazon EBS) untuk membuat dan mengelola volume tersebut. EBS mengenkripsi kunci data volume Anda menggunakan algoritme AES-256 standar industri. Untuk informasi selengkapnya, lihat Enkripsi Amazon EBS di Panduan Pengguna Amazon EC2 User Guide untuk Instans Windows.

Enkripsi dalam transit

Untuk PCoIP, data dalam transit dienkripsi menggunakan enkripsi TLS 1.2 dan penandatanganan permintaan SigV4. Protokol PCoIP menggunakan lalu lintas UDP terenkripsi, dengan enkripsi AES, untuk piksel streaming. hubungan streaming, menggunakan port 4172 (TCP dan UDP), dienkripsi dengan menggunakan cipher AES-128 dan AES-256, tetapi enkripsi default ke 128-bit. Anda dapat mengubah default ini menjadi 256-bit, baik dengan menggunakan pengaturan Kebijakan Grup Pengaturan Keamanan PCoIP untuk Windows WorkSpaces, atau dengan memodifikasi Pengaturan Keamanan PCoIP dalam file untuk Amazon Linux. `pcoip-agent.conf` WorkSpaces

Untuk mempelajari selengkapnya tentang Administrasi Kebijakan Grup untuk Amazon WorkSpaces, lihat Konfigurasikan pengaturan keamanan PCoIP diKelola Windows Anda WorkSpaces. Untuk mempelajari selengkapnya tentang memodifikasi file `pcoip-agent.conf`, lihat Kontrol perilaku Agen PCoIP di Amazon Linux WorkSpaces dan Pengaturan Keamanan PCoIP dalam dokumentasi Teradici.

Untuk WorkSpaces Streaming Protocol (WSP), streaming dan kontrol data dalam transit dienkripsi menggunakan enkripsi DTLS 1.2 untuk lalu lintas UDP dan enkripsi TLS 1.2 untuk lalu lintas TCP, dengan cipher AES-256.

Identitas dan manajemen akses untuk WorkSpaces

Secara default, pengguna IAM tidak memiliki izin untuk WorkSpaces sumber daya dan operasi. Untuk mengizinkan pengguna IAM mengelola WorkSpaces sumber daya, Anda harus membuat kebijakan IAM yang secara eksplisit memberi mereka izin, dan melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk memberikan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup diAWS IAM Identity Center:

  Buat set izin. Ikuti petunjuk di Buat set izin di Panduan AWS IAM Identity Center Pengguna.
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti petunjuk dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diasumsikan pengguna Anda. Ikuti petunjuk dalam Membuat peran untuk pengguna IAM di Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk di Menambahkan izin ke pengguna (konsol) di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang kebijakan IAM, lihat Izin dan Kebijakan dalam Panduan Pengguna IAM.

WorkSpaces juga menciptakan peran IAM,`workspaces_DefaultRole`, yang memungkinkan akses WorkSpaces layanan ke sumber daya yang diperlukan.

Untuk informasi selengkapnya tentang IAM, lihat Identity and Access Management (IAM) di Panduan Pengguna IAM. Anda dapat menemukan kunci konteks sumber daya, tindakan, dan kondisi WorkSpaces khusus untuk digunakan dalam kebijakan izin IAM di Kunci Tindakan, Sumber Daya, dan Kondisi untuk Amazon WorkSpaces di Panduan Pengguna IAM.

Untuk alat yang membantu Anda membuat kebijakan IAM, lihat Generator AWS Kebijakan. Anda juga dapat menggunakan Simulator Kebijakan IAM untuk menguji apakah kebijakan mengizinkan atau menolak permintaan khusus ke AWS.

> **Note**
>
> Amazon WorkSpaces tidak mendukung penyediaan kredensional IAM ke dalam WorkSpace (seperti dengan profil instance).

Daftar Isi

Contoh kebijakan

Contoh berikut menunjukkan pernyataan kebijakan yang dapat Anda gunakan untuk mengontrol izin yang dimiliki pengguna IAM ke Amazon. WorkSpaces

Example 1: Lakukan semua WorkSpaces tugas

Pernyataan kebijakan berikut memberikan izin pengguna IAM untuk melakukan semua WorkSpaces tugas, termasuk membuat dan mengelola direktori. Hal ini juga memberikan izin untuk menjalankan prosedur pengaturan cepat.

Meskipun Amazon WorkSpaces sepenuhnya mendukung `Action` dan `Resource` elemen saat menggunakan API dan alat baris perintah, untuk menggunakan Amazon WorkSpaces dariAWS Management Console, pengguna IAM harus memiliki izin untuk tindakan dan sumber daya berikut:

- Tindakan: `"workspaces:*"` dan `"ds:*"`
- Sumber Daya: `"Resource": "*"`

Contoh kebijakan berikut menunjukkan cara mengizinkan pengguna IAM untuk menggunakan Amazon WorkSpaces dari. AWS Management Console

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
```

```
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Example 2: Lakukan WorkSpace tugas-tugas khusus

Pernyataan kebijakan berikut memberikan izin pengguna IAM untuk melakukan tugas WorkSpace -spesifik, seperti meluncurkan dan menghapus. WorkSpaces Dalam pernyataan kebijakan, `ds:*` memberikan izin yang luas — kontrol penuh atas semua objek Directory Services di akun.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Untuk juga memberikan pengguna kemampuan untuk mengaktifkan Amazon WorkDocs bagi pengguna di dalamnya WorkSpaces, tambahkan `workdocs` operasi yang ditunjukkan dalam contoh berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

Untuk juga memberikan pengguna kemampuan untuk menggunakan WorkSpaces wizard Peluncuran, tambahkan kms operasi seperti yang ditunjukkan pada contoh berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3: Lakukan semua WorkSpaces tugas untuk BYOL WorkSpaces

Pernyataan kebijakan berikut memberikan izin kepada pengguna IAM untuk melakukan semua WorkSpaces tugas, termasuk tugas Amazon EC2 yang diperlukan untuk membuat Bring Your Own License (BYOL). WorkSpaces

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
```

```
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Tentukan WorkSpaces sumber daya dalam kebijakan IAM

Untuk menentukan WorkSpaces sumber daya dalam `Resource` elemen pernyataan kebijakan, gunakan Amazon Resource Name (ARN) sumber daya. Anda mengontrol akses ke WorkSpaces sumber daya dengan mengizinkan atau menolak izin untuk menggunakan tindakan API yang ditentukan dalam `Action` elemen pernyataan kebijakan IAM Anda. WorkSpaces mendefinisikan ARN untuk WorkSpaces, bundel, grup IP, dan direktori.

WorkSpace ARN

WorkSpace ARN memiliki sintaks yang ditunjukkan dalam contoh berikut.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

wilayah

Wilayah tempat WorkSpace berada (misalnya,`us-east-1`).

account_id

ID akun AWS tanpa tanda hubung (misalnya, `123456789012`).

workspace_identifier

ID dari WorkSpace (misalnya,`ws-a1bcd2efg`).

Berikut ini adalah format `Resource` elemen pernyataan kebijakan yang mengidentifikasi spesifik WorkSpace.

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

Anda dapat menggunakan * wildcard untuk menentukan semua WorkSpaces yang dimiliki akun tertentu di Wilayah tertentu.

ARN citra

Sebuah WorkSpace gambar ARN memiliki sintaks yang ditunjukkan dalam contoh berikut.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

wilayah

Wilayah tempat WorkSpace gambar berada (misalnya,`us-east-1`).

account_id

ID akun AWS tanpa tanda hubung (misalnya, `123456789012`).

bundle_identifier

ID WorkSpace gambar (misalnya,`wsi-a1bcd2efg`).

Berikut ini adalah format elemen `Resource` pernyataan kebijakan yang mengidentifikasi citra tertentu.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

Anda dapat menggunakan wildcard * untuk menentukan semua citra milik akun tertentu dalam Wilayah tertentu.

ARN Paket

ARN Paket memiliki sintaksis yang ditunjukkan dalam contoh berikut.

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

wilayah

Wilayah tempat WorkSpace berada (misalnya,`us-east-1`).

account_id

ID akun AWS tanpa tanda hubung (misalnya, `123456789012`).

bundle_identifier

ID WorkSpace bundel (misalnya,`wsb-a1bcd2efg`).

Berikut ini adalah format elemen `Resource` pernyataan kebijakan yang mengidentifikasi paket tertentu.

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

Anda dapat menggunakan wildcard * untuk menentukan semua paket milik akun tertentu dalam Wilayah tertentu.

ARN Grup IP

ARN Grup IP memiliki sintaksis yang ditunjukkan dalam contoh berikut.

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

wilayah

Wilayah tempat WorkSpace berada (misalnya,`us-east-1`).

account_id

ID akun AWS tanpa tanda hubung (misalnya, `123456789012`).

ipgroup_identifier

ID dari grup IP (misalnya, `wsipg-a1bcd2efg`).

Berikut ini adalah format elemen `Resource` pernyataan kebijakan yang mengidentifikasi grup IP tertentu.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

Anda dapat menggunakan wildcard * untuk menentukan semua grup IP milik akun tertentu dalam Wilayah tertentu.

ARN Direktori

Sebuah direktori ARN memiliki sintaksis yang ditunjukkan dalam contoh berikut.

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

wilayah

Wilayah tempat WorkSpace berada (misalnya,`us-east-1`).

account_id

ID akun AWS tanpa tanda hubung (misalnya, `123456789012`).

directory_identifier

ID direktori (misalnya, `d-12345a67b8`).

Berikut ini adalah format elemen `Resource` pernyataan kebijakan yang mengidentifikasi direktori tertentu.

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

Anda dapat menggunakan wildcard `*` untuk menentukan semua direktori milik akun tertentu dalam Wilayah tertentu.

ARN alias hubungan

ARN alias hubungan memiliki sintaksis yang ditunjukkan dalam contoh berikut.

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

wilayah

Wilayah tempat hubungan alias berada (misalnya, `us-east-1`).

account_id

ID akun AWS tanpa tanda hubung (misalnya, `123456789012`).

connectionalias_identifier

ID dari alias hubungan (misalnya, `wsca-12345a67b8`).

Berikut ini adalah format elemen `Resource` pernyataan kebijakan yang mengidentifikasi alias hubungan tertentu.

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

Anda dapat menggunakan wildcard `*` untuk menentukan semua alias hubungan milik akun tertentu dalam Wilayah tertentu.

Tindakan API yang tidak memiliki dukungan untuk izin di tingkat sumber daya

Anda tidak dapat menentukan sumber daya ARN dengan tindakan API berikut:

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

Untuk tindakan API yang tidak mendukung izin tingkat sumber daya, Anda harus menetapkan pernyataan sumber daya yang ditunjukkan dalam contoh berikut.

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

Tindakan API yang tidak mendukung pembatasan tingkat akun pada sumber daya bersama

Untuk tindakan API berikut, Anda tidak dapat menentukan ID akun di ARN sumber daya saat sumber daya tidak dimiliki oleh akun:

- AssociateConnectionAlias
- CopyWorkspaceImage
- DisassociateConnectionAlias

Untuk tindakan API ini, Anda dapat menentukan ID akun di ARN sumber daya hanya ketika akun memiliki sumber daya untuk ditindaklanjuti. Bila akun tidak memiliki sumber daya, Anda harus menentukan * untuk ID akun, seperti yang ditunjukkan dalam contoh berikut.

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

Buat ruang kerja_ DefaultRole Peran

Sebelum Anda dapat mendaftarkan direktori menggunakan API, Anda harus memverifikasi bahwa peran bernama `workspaces_DefaultRole` ada. Peran ini dibuat oleh Pengaturan Cepat atau jika Anda meluncurkan WorkSpace menggunakanAWS Management Console, dan itu memberikan WorkSpaces izin Amazon untuk mengakses AWS sumber daya tertentu atas nama Anda. Jika peran ini tidak ada, Anda dapat membuatnya menggunakan prosedur berikut.

Untuk membuat peran ruang kerja_ DefaultRole

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Pada panel navigasi di sebelah kiri, pilih Peran.
3. Pilih Create role (Buat peran).
4. Di Pilih tipe entitas terpercaya, pilih Akun AWS lain.
5. Untuk ID Akun, masukkan ID akun Anda tanpa tanda hubung atau spasi.
6. Untuk Opsi, jangan tentukan Autentikasi Multi-Faktor (MFA).
7. Pilih Selanjutnya: Izin.
8. Pada halaman Lampirkan kebijakan izin, pilih kebijakan AWS terkelola AmazonWorkSpacesServiceAccessdan AmazonWorkSpacesSelfServiceAccess.
9. Di bawah Setel batas izin, sebaiknya Anda tidak menggunakan batas izin karena potensi konflik dengan kebijakan yang dilampirkan pada peran ini. Konflik tersebut dapat memblokir izin tertentu yang diperlukan untuk peran tersebut.
10. Pilih Selanjutnya: Tanda.
11. Pada halaman Tambahkan tanda (opsional), tambahkan tanda jika diperlukan.
12. Pilih Selanjutnya: Tinjau.
13. Pada halaman Tinjau, untuk Nama peran, masukkan **`workspaces_DefaultRole`**.
14. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.

15. Pilih Buat Peran.
16. Pada halaman Ringkasan untuk DefaultRole peran workspaces_, pilih tab Trust relationship.
17. Pilih tab Hubungan Kepercayaan, pilih Edit Hubungan Kepercayaan.
18. Pada halaman Edit Hubungan kepercayaan, gantikan pernyataan kebijakan yang ada dengan pernyataan berikut.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. Pilih Perbarui Kebijakan Kepercayaan.

Buat peran layanan AmazonWorkSpaces PCAAccess

Sebelum pengguna dapat masuk menggunakan otentikasi berbasis sertifikat, Anda harus memverifikasi bahwa peran bernama ada. `AmazonWorkSpacesPCAAccess` Peran ini dibuat saat Anda mengaktifkan otentikasi berbasis sertifikat pada Direktori menggunakanAWS Management Console, dan memberikan WorkSpaces izin Amazon untuk mengakses AWS Private CA sumber daya atas nama Anda. Jika peran ini tidak ada karena Anda tidak menggunakan konsol untuk mengelola otentikasi berbasis sertifikat, Anda dapat membuatnya menggunakan prosedur berikut.

Untuk membuat peran layanan AmazonWorkSpaces PCAAccess menggunakan AWS CLI

1. Buat file JSON bernama `AmazonWorkSpacesPCAAccess.json` dengan teks berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Sesuaikan `AmazonWorkSpacesPCAAccess.json` jalur sesuai kebutuhan dan jalankan AWS CLI perintah berikut untuk membuat peran layanan dan melampirkan kebijakan terkelola AmazonWorkspacesPCAAccess.

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

AWSkebijakan terkelola untuk WorkSpaces

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

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

Selain itu, AWS mendukung kebijakan-kebijakan terkelola untuk fungsi tugas yang mencakup beberapa layanan. Misalnya, kebijakan `ReadOnlyAccess` AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS menambahkan izin hanya-baca untuk operasi dan sumber daya yang baru. Untuk melihat daftar dan

deskripsi dari kebijakan-kebijakan fungsi tugas, lihat kebijakan terkelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWSkebijakan terkelola: AmazonWorkSpacesAdmin

Kebijakan ini menyediakan akses ke tindakan WorkSpaces administratif Amazon. Ini memberikan izin berikut:

- `workspaces`- Memungkinkan akses untuk melakukan tindakan administratif pada WorkSpaces sumber daya.
- `kms`- Memungkinkan akses ke daftar dan menggambarkan kunci KMS, serta daftar alias.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
                "workspaces:StartWorkspaces",
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWSkebijakan terkelola: AmazonWorkspaces PCAAccess

Kebijakan terkelola ini menyediakan akses ke sumber daya AWS Certificate Manager Private Certificate Authority (Private CA) di AWS akun Anda untuk otentikasi berbasis sertifikat. Ini termasuk dalam peran AmazonWorkSpaces PCAAccess, dan memberikan izin berikut:

- `acm-pca`- Memungkinkan akses ke AWS Private CA untuk mengelola otentikasi berbasis sertifikat.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}
```

AWSkebijakan terkelola: AmazonWorkSpacesSelfServiceAccess

Kebijakan ini menyediakan akses ke WorkSpaces layanan Amazon untuk melakukan tindakan WorkSpaces layanan mandiri yang dimulai oleh pengguna. Ini termasuk dalam `workspaces_DefaultRole` peran, dan memberikan izin berikut:

- `workspaces`- Memungkinkan akses ke kemampuan WorkSpaces manajemen swalayan untuk pengguna.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWSkebijakan terkelola: AmazonWorkSpacesServiceAccess

Kebijakan ini menyediakan akses akun pelanggan ke WorkSpaces layanan Amazon untuk meluncurkan file WorkSpace. Ini termasuk dalam `workspaces_DefaultRole` peran, dan memberikan izin berikut:

- `ec2`- Memungkinkan akses untuk mengelola sumber daya Amazon EC2 yang terkait dengan WorkSpace, seperti antarmuka jaringan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

WorkSpaces pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola WorkSpaces sejak layanan ini mulai melacak perubahan ini.

Perubahan	Deskripsi	Tanggal
the section called “AmazonWorkSpacesAdmin”- Kebijakan yang diperbarui	WorkSpaces menambahkan `workspaces:RestoreWorkspace` tindakan ke kebijakan WorkSpacesAdmin terkelola Amazon, memberikan akses admin untuk memulihkan. WorkSpaces	Juni 25, 2023
the section called “AmazonWorkspacesPCAAccess”- Ditambahkan kebijakan baru	WorkSpaces menambahkan kebijakan terkelola baru untuk memberikan `acm-pca` izin mengelola AWS Private CA untuk mengelola otentikasi berbasis sertifikat.	November 18, 2022
WorkSpaces mulai melacak perubahan	WorkSpaces mulai melacak perubahan untuk kebijakan yang WorkSpaces dikelola.	1 Maret 2021

Validasi kepatuhan untuk Amazon WorkSpaces

Auditor pihak ketiga menilai keamanan dan kepatuhan Amazon WorkSpaces sebagai bagian dari beberapa program AWS kepatuhan. Ini mencakup SOC, PCI, FedRAMP, HIPAA, dan sebagainya.

Untuk daftar layanan AWS dalam cakupan program kepatuhan tertentu, lihat Layanan AWS dalam Cakupan berdasarkan Program Kepatuhan. Untuk informasi umum, lihat Program Kepatuhan AWS.

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

Untuk informasi lebih lanjut tentang WorkSpaces dan FedRAMP, lihat. Siapkan Amazon WorkSpaces untuk otorisasi FedRAMP atau kepatuhan DoD SRG

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

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah untuk deployment lingkungan dasar yang fokus pada keamanan dan kepatuhan di AWS.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang sesuai dengan HIPAA.
- Sumber Daya Kepatuhan AWS – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan Developer AWS Config – AWS Config; menilai seberapa patuh konfigurasi sumber daya Anda terhadap praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub – Layanan AWS ini akan menyediakan tampilan komprehensif status keamanan dalam AWS yang akan membantu Anda dalam memeriksa kepatuhan terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di Amazon WorkSpaces

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

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

Amazon WorkSpaces juga menyediakan pengalihan lintas wilayah, fitur yang berfungsi dengan kebijakan perutean failover Sistem Nama Domain (DNS) Anda untuk mengarahkan WorkSpaces

pengguna Anda ke alternatif WorkSpaces di AWS Wilayah lain saat primer mereka tidak tersedia. WorkSpaces Untuk informasi selengkapnya, lihat Pengalihan Lintas Wilayah untuk Amazon WorkSpaces.

Keamanan infrastruktur di Amazon WorkSpaces

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

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

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Cipher suite dengan perfect forward secrecy (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

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

Isolasi jaringan

Cloud Privat Virtual (VPC) adalah jaringan virtual dalam area Anda yang diisolasi secara logis dalam AWS Cloud. Anda dapat menerapkan subnet pribadi WorkSpaces di VPC Anda. Untuk informasi selengkapnya, lihat Konfigurasikan VPC untuk WorkSpaces.

Untuk mengizinkan lalu lintas hanya dari rentang alamat tertentu (misalnya, dari jaringan perusahaan Anda), perbarui grup keamanan untuk VPC Anda atau gunakan Grup kontrol akses IP.

Anda dapat membatasi WorkSpace akses ke perangkat tepercaya dengan sertifikat yang valid. Untuk informasi selengkapnya, lihat Batasi WorkSpaces akses ke perangkat tepercaya.

Isolasi pada host fisik

Berbeda WorkSpaces pada inang fisik yang sama diisolasi satu sama lain melalui hypervisor. Seolah-olah WorkSpaces berada di host fisik yang terpisah. Ketika a WorkSpace dihapus, memori yang dialokasikan untuk itu digosok (diatur ke nol) oleh hypervisor sebelum dialokasikan ke yang baru. WorkSpace

Otorisasi pengguna perusahaan

Dengan WorkSpaces, direktori dikelola melalui. AWS Directory Service Anda dapat membuat direktori, yang dikelola secara mandiri untuk pengguna. Atau Anda dapat berintegrasi dengan lingkungan Direktori Aktif yang tersedia sehingga pengguna Anda dapat menggunakan kredensialnya saat ini untuk mendapatkan akses tanpa batas ke sumber daya perusahaan. Untuk informasi selengkapnya, lihat Kelola direktori untuk WorkSpaces.

Untuk lebih mengontrol akses ke Anda WorkSpaces, gunakan otentikasi multi-faktor. Untuk informasi selengkapnya, lihat Cara Mengaktifkan Autentikasi Multi-Faktor untuk Layanan AWS.

Membuat permintaan Amazon WorkSpaces API melalui titik akhir antarmuka VPC

Anda dapat terhubung langsung ke titik akhir Amazon WorkSpaces API melalui titik akhir antarmuka di cloud pribadi virtual (VPC) Anda alih-alih terhubung melalui internet. Saat Anda menggunakan titik akhir antarmuka VPC, komunikasi antara VPC dan titik akhir Amazon WorkSpaces API dilakukan sepenuhnya dan aman di dalam jaringan. AWS

> **Note**
>
> Fitur ini hanya dapat digunakan untuk menghubungkan ke titik akhir WorkSpaces API. Untuk terhubung WorkSpaces menggunakan WorkSpaces klien, konektivitas internet diperlukan, seperti yang dijelaskan dalamAlamat IP dan persyaratan port untuk WorkSpaces.

Titik akhir Amazon WorkSpaces API mendukung titik akhir antarmuka Amazon Virtual Private Cloud (Amazon VPC) yang didukung oleh. AWS PrivateLink Masing-masing VPC endpoint diwakili oleh satu atau lebih antarmuka jaringan (juga dikenal sebagai antarmuka jaringan elastis, atau ENI) dengan alamat IP privat di subnet VPC Anda.

Titik akhir antarmuka VPC menghubungkan VPC Anda langsung ke titik akhir Amazon WorkSpaces API tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan titik akhir WorkSpaces Amazon API.

Anda dapat membuat titik akhir antarmuka untuk terhubung ke Amazon WorkSpaces dengan perintah AWS Management Console or AWS Command Line Interface (AWS CLI). Untuk instruksi, lihat Membuat Titik Akhir Antarmuka.

Setelah Anda membuat titik akhir VPC, Anda dapat menggunakan contoh perintah CLI berikut yang menggunakan `endpoint-url` parameter untuk menentukan titik akhir antarmuka ke titik akhir Amazon API: WorkSpaces

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com

aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

Jika Anda mengaktifkan nama host DNS privat untuk VPC endpoint, Anda tidak perlu menentukan titik akhir URL. Nama host DNS Amazon WorkSpaces API yang digunakan CLI dan Amazon WorkSpaces SDK secara default (https://api.workspaces. *Region* .amazonaws.com) menyelesaikan ke titik akhir VPC Anda.

Titik akhir Amazon WorkSpaces API mendukung titik akhir VPC di AWS semua Wilayah di mana Amazon VPC dan Amazon tersedia. WorkSpaces Amazon WorkSpaces mendukung panggilan ke semua API publiknya di dalam VPC Anda.

Untuk mempelajari selengkapnya tentang AWS PrivateLink, lihat AWS PrivateLink dokumentasi. Untuk harga VPC endpoints, lihat Harga VPC. Untuk mempelajari selengkapnya tentang VPC dan titik akhir, lihat Amazon VPC.

Untuk melihat daftar titik akhir Amazon WorkSpaces API menurut Wilayah, lihat Titik Akhir WorkSpaces API.

> **Note**
>
> Titik akhir Amazon WorkSpaces API dengan tidak AWS PrivateLink didukung untuk titik akhir Amazon WorkSpaces API Federal Information Processing Standard (FIPS).

Membuat kebijakan titik akhir VPC untuk Amazon WorkSpaces

Anda dapat membuat kebijakan untuk titik akhir Amazon VPC untuk Amazon WorkSpaces untuk menentukan hal berikut:

- Principal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang dapat digunakan untuk mengambil tindakan.

Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan VPC Endpoint dalam Panduan Pengguna Amazon VPC.

> **Note**
>
> Kebijakan titik akhir VPC tidak didukung untuk titik akhir Amazon Federal Information Processing Standard (FIPS). WorkSpaces

Contoh kebijakan titik akhir VPC berikut menetapkan bahwa semua pengguna yang memiliki akses ke titik akhir antarmuka VPC diizinkan untuk memanggil titik akhir yang dihosting Amazon bernama. WorkSpaces `ws-f9abcdefg`

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
     ]
```

```
}
```

Dalam contoh ini, tindakan berikut ditolak:

- Memanggil titik akhir yang WorkSpaces dihosting Amazon selain. `ws-f9abcdefg`
- Melakukan tindakan pada sumber daya apa pun selain yang ditentukan (WorkSpace ID:`ws-f9abcdefg`).

> **Note**
>
> Dalam contoh ini, pengguna masih dapat mengambil tindakan Amazon WorkSpaces API lainnya dari luar VPC. Untuk membatasi panggilan API ke panggilan dari dalam VPC, Identitas dan manajemen akses untuk WorkSpaces lihat informasi tentang penggunaan kebijakan berbasis identitas untuk mengontrol akses ke titik akhir Amazon API. WorkSpaces

Hubungkan jaringan pribadi Anda ke VPC

Untuk memanggil Amazon WorkSpaces API melalui VPC Anda, Anda harus terhubung dari instance yang ada di dalam VPC, atau menghubungkan jaringan pribadi Anda ke VPC Anda dengan menggunakan () atau. AWS Virtual Private Network AWS VPN AWS Direct Connect Untuk informasi selengkapnya, lihat Koneksi VPN di Panduan Pengguna Amazon Virtual Private Cloud. Untuk informasi tentang AWS Direct Connect, lihat Membuat hubungan di Panduan Pengguna AWS Direct Connect.

Perbarui manajemen di WorkSpaces

Kami menyarankan Anda secara teratur menambal, memperbarui, dan mengamankan sistem operasi dan aplikasi Anda WorkSpaces. Anda dapat mengonfigurasi WorkSpaces untuk diperbarui WorkSpaces selama jendela pemeliharaan rutin atau Anda dapat memperbaruinya sendiri. Untuk informasi selengkapnya, lihat WorkSpace pemeliharaan.

Untuk aplikasi di Anda WorkSpaces, Anda dapat menggunakan layanan pembaruan otomatis yang disediakan atau mengikuti rekomendasi untuk menginstal pembaruan yang disediakan oleh vendor aplikasi.

Memecahkan masalah WorkSpaces

Informasi berikut dapat membantu Anda memecahkan masalah dengan Anda. WorkSpaces

Mengaktifkan pencatatan lanjutan

Untuk membantu memecahkan masalah yang mungkin dialami pengguna, Anda dapat mengaktifkan pencatatan lanjutan pada klien Amazon WorkSpaces mana pun.

Pendataan lanjutan menghasilkan berkas log yang berisi informasi diagnostik dan detail tingkat debugging, termasuk data performa verbose. Untuk 1.0+ dan 2.0+ klien, file logging lanjutan ini secara otomatis diunggah ke database di. AWS

> **Note**
>
> Untuk mendapatkan AWS ulasan file logging lanjutan, dan untuk menerima dukungan teknis untuk masalah dengan WorkSpaces klien Anda, hubungi AWS Support. Untuk informasi lebih lanjut, lihat AWS Support Pusat.

Untuk mengaktifkan pencatatan lanjutan untuk Akses Web

Untuk mengaktifkan pencatatan lanjutan untuk Akses Web

1. Buka klien Amazon WorkSpaces Web Access Anda.
2. Di bagian atas halaman WorkSpaces masuk, pilih Pencatatan diagnostik.
3. Di kotak dialog pop-up, pastikan bahwa Pencatatan diagnostik diaktifkan.
4. Untuk tingkat Log, pilih Pencatatan lanjutan.

Untuk mengakses file log di Google Chrome, Microsoft Edge, dan Firefox

1. Buka menu konteks (klik kanan) pada browser atau tekan Ctrl + Shift+I (atau untuk Mac, perintah + opsi+I) pada keyboard Anda untuk membuka panel alat pengembang.
2. Di panel alat pengembang, pilih tab Konsol untuk menemukan file log.

Untuk mengakses file log di Safari

1. Pilih Safari, Pengaturan.
2. Di jendela Pengaturan, pilih tab Advanced.
3. Pilih Tampilkan menu Kembangkan di bilah menu.
4. Dari tab Develop di menu bar, pilih Develop > Show Web Inspector.
5. Di panel Safari Web Inspector, pilih tab Console untuk menemukan file log.

Untuk mengaktifkan pencatatan lanjutan untuk 4.0+ klien

Log klien Windows disimpan di lokasi berikut:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Untuk mengaktifkan log lanjutan untuk klien Windows

1. Tutup WorkSpaces klien Amazon.
2. Buka Aplikasi Prompt Perintah.
3. Luncurkan WorkSpaces klien dengan `-l3` bendera.

```
c:

cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> Jika WorkSpaces diinstal untuk satu pengguna dan tidak semua pengguna, gunakan perintah berikut:
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> workspaces.exe -l3
> ```

Log klien macOS disimpan di lokasi berikut:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

Untuk mengaktifkan log lanjutan untuk klien macOS

1. Tutup WorkSpaces klien Amazon.
2. Buka Terminal.
3. Jalankan perintah berikut.

   ```
   open -a workspaces --args -l3
   ```

Untuk mengaktifkan pencatatan lanjutan untuk klien Android

1. Tutup WorkSpaces klien Amazon.
2. Buka menu klien Android.
3. Pilih Support.
4. Pilih pengaturan Logging.
5. Pilih Aktifkan pencatatan lanjutan.

Untuk mengambil log untuk klien Android setelah mengaktifkan pencatatan lanjutan:

- Pilih Ekstrak log untuk menyimpan log zip secara lokal.

Log klien Linux disimpan di lokasi berikut:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Untuk mengaktifkan log lanjutan untuk klien Linux

1. Tutup WorkSpaces klien Amazon.
2. Buka Terminal.
3. Jalankan perintah berikut.

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

Untuk mengaktifkan pencatatan lanjutan untuk 3.0 klien

Log klien Windows disimpan di lokasi berikut:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Untuk mengaktifkan log lanjutan untuk klien Windows

1. Tutup WorkSpaces klien Amazon.
2. Buka Aplikasi Prompt Perintah.
3. Luncurkan WorkSpaces klien dengan `-l3` bendera.

   ```
   c:

   cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

   workspaces.exe -l3
   ```

   > **Note**
   >
   > Jika WorkSpaces diinstal untuk satu pengguna dan tidak semua pengguna, gunakan perintah berikut:
   >
   > ```
   > c:
   > cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   > workspaces.exe -l3
   > ```

Log klien macOS disimpan di lokasi berikut:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

Untuk mengaktifkan log lanjutan untuk klien macOS

1. Tutup WorkSpaces klien Amazon.
2. Buka Terminal.
3. Jalankan perintah berikut.

   ```
   open -a workspaces --args -l3
   ```

Untuk mengaktifkan pencatatan lanjutan untuk klien Android

1. Tutup WorkSpaces klien Amazon.
2. Buka menu klien Android.
3. Pilih Support.
4. Pilih pengaturan Logging.
5. Pilih Aktifkan pencatatan lanjutan.

Untuk mengambil log untuk klien Android setelah mengaktifkan pencatatan lanjutan:

- Pilih Ekstrak log untuk menyimpan log zip secara lokal.

Log klien Linux disimpan di lokasi berikut:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Untuk mengaktifkan log lanjutan untuk klien Linux

1. Tutup WorkSpaces klien Amazon.
2. Buka Terminal.
3. Jalankan perintah berikut.

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

Untuk mengaktifkan log lanjutan untuk klien 1.0+ dan 2.0+

1. Buka WorkSpaces klien.
2. Pilih ikon gear di sudut kanan atas aplikasi klien.
3. Pilih Pengaturan Lanjutan.
4. Pilih kotak centang Aktifkan Log Lanjutan.
5. Pilih Simpan.

Log klien Windows disimpan di lokasi berikut:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

Log klien macOS disimpan di lokasi berikut:

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

Pecahkan masalah tertentu

Informasi berikut dapat membantu Anda memecahkan masalah tertentu dengan Anda. WorkSpaces

Masalah

- Saya tidak dapat membuat Amazon Linux WorkSpace karena ada karakter yang tidak valid di nama pengguna
- Saya mengubah shell untuk Amazon Linux saya WorkSpace dan sekarang saya tidak dapat menyediakan sesi PCoIP
- Linux Amazon saya WorkSpaces tidak akan mulai
- Peluncuran WorkSpaces di direktori saya yang terhubung sering gagal
- Peluncuran WorkSpaces gagal dengan kesalahan internal
- Ketika saya mencoba untuk mendaftar direktori, pendaftaran gagal dan meninggalkan direktori dalam keadaan KESALAHAN
- Pengguna saya tidak dapat terhubung ke Windows WorkSpace dengan spanduk masuk interaktif
- Pengguna saya tidak dapat terhubung ke Windows WorkSpace
- Pengguna saya mengalami masalah ketika mereka mencoba masuk WorkSpaces dari Akses WorkSpaces Web
- WorkSpaces Klien Amazon menampilkan layar abu-abu “Memuat...” untuk sementara waktu sebelum kembali ke layar login. Tidak ada pesan kesalahan lain yang muncul.
- Pengguna saya menerima pesan "WorkSpace Status: Tidak sehat. Kami tidak dapat menghubungkan Anda dengan Anda WorkSpace. Coba lagi dalam beberapa menit."
- Pengguna saya menerima pesan “Perangkat ini tidak diizinkan untuk mengakses WorkSpace. Hubungi administrator Amazon WorkDocs Anda untuk bantuan."
- Pengguna saya menerima pesan "Tidak ada jaringan. Hubungan jaringan hilang. Periksa hubungan jaringan Anda atau hubungi administrator Anda untuk mendapatkan bantuan." saat mencoba terhubung ke WSP WorkSpace
- WorkSpaces Klien memberi pengguna saya kesalahan jaringan, tetapi mereka dapat menggunakan aplikasi lain yang mendukung jaringan di perangkat mereka

- WorkSpace Pengguna saya melihat pesan galat berikut: “Perangkat tidak dapat terhubung ke layanan pendaftaran. Periksa pengaturan jaringan Anda."
- Pengguna klien nol PCoIP menerima kesalahan "Sertifikat yang disediakan tidak valid karena timestamp"
- Printer USB dan periferal USB lainnya tidak bekerja untuk klien nol PCoIP
- Pengguna saya melewatkan pembaruan aplikasi klien Windows atau macOS mereka dan tidak diminta untuk menginstal versi terbaru
- Pengguna saya tidak dapat memasang aplikasi klien Android di Chromebook mereka
- Pengguna saya tidak menerima email undangan atau email pengaturan ulang kata sandi
- Pengguna saya tidak melihat opsi Lupa kata sandi? pada layar masuk klien
- Saya menerima pesan “Administrator sistem telah menetapkan kebijakan untuk mencegah instalasi ini” ketika saya mencoba menginstal aplikasi pada Windows WorkSpace
- Tidak ada WorkSpaces di direktori saya yang dapat terhubung ke internet
- Saya WorkSpace telah kehilangan akses internetnya
- Saya menerima kesalahan "DNS tidak tersedia" ketika mencoba menghubungkan ke direktori on-premise saya
- Saya menerima kesalahan "Masalah hubungan terdeteksi" ketika mencoba menghubungkan ke direktori on-premise saya
- Saya menerima kesalahan "catatan SRV" ketika mencoba menghubungkan ke direktori on-premise saya
- WorkSpace Jendela saya tertidur ketika dibiarkan menganggur
- Salah satu dari saya WorkSpaces memiliki keadaan UNHEALTHY
- Saya WorkSpace tiba-tiba mogok atau reboot
- Nama pengguna yang sama memiliki lebih dari satu WorkSpace, tetapi pengguna hanya dapat masuk ke salah satu WorkSpaces
- Saya mengalami masalah dalam menggunakan Docker dengan Amazon WorkSpaces
- Saya menerima ThrottlingException kesalahan pada beberapa panggilan API saya
- Saya WorkSpace terus terputus ketika saya membiarkannya berjalan di latar belakang
- Federasi SAFL 2.0 tidak berfungsi. Pengguna saya tidak berwenang untuk melakukan streaming WorkSpaces desktop mereka.
- Pengguna saya terputus dari WorkSpaces sesi mereka setiap 60 menit.

- Pengguna saya mendapatkan kesalahan URI pengalihan ketika mereka melakukan federasi menggunakan aliran yang dimulai oleh penyedia identitas SAMP 2.0 (iDP), atau instance tambahan dari aplikasi WorkSpaces klien dimulai setiap kali pengguna saya mencoba masuk dari klien setelah federasi ke iDP.
- Pengguna saya menerima pesan, “Ada yang tidak beres: Terjadi kesalahan saat meluncurkan WorkSpace" ketika mereka mencoba masuk ke aplikasi WorkSpaces klien setelah federasi ke iDP.
- Pengguna saya menerima pesan, “Tidak dapat memvalidasi tag” ketika mereka mencoba masuk ke aplikasi WorkSpaces klien setelah federasi ke iDP.
- Pengguna saya menerima pesan, “Klien dan server tidak dapat berkomunikasi, karena mereka tidak memiliki algoritma umum”.
- Mikrofon atau kamera web saya tidak berfungsi di Windows WorkSpaces.
- Pengguna saya tidak dapat masuk menggunakan otentikasi berbasis sertifikat dan diminta untuk kata sandi baik di WorkSpaces klien atau layar masuk Windows saat mereka terhubung ke sesi desktop mereka.
- Saya mencoba melakukan sesuatu yang membutuhkan media instalasi Windows tetapi WorkSpaces tidak menyediakannya.
- Saya ingin meluncurkan WorkSpaces dengan Direktori AWS Terkelola yang ada yang dibuat di WorkSpaces Wilayah yang tidak didukung.
- Saya ingin memperbarui Firefox di Amazon Linux 2.
- Pengguna saya dapat mengatur ulang kata sandi mereka menggunakan WorkSpaces klien, mengabaikan pengaturan Fine Grained Password Policy (FFGP) yang dikonfigurasi. AWS Managed Microsoft AD

Saya tidak dapat membuat Amazon Linux WorkSpace karena ada karakter yang tidak valid di nama pengguna

Untuk Amazon Linux WorkSpaces, nama pengguna:

- Dapat berisi maksimal 20 karakter
- Dapat berisi huruf, spasi, dan angka yang dapat mewakili dalam UTF-8
- Dapat menyertakan karakter berikut ini: _.-#
- Tidak dapat memulai dengan simbol tanda hubung (-) sebagai karakter pertama dari nama pengguna

> **Note**
>
> Keterbatasan ini tidak berlaku untuk Windows WorkSpaces. Windows WorkSpaces mendukung simbol @ dan - untuk semua karakter dalam nama pengguna.

Saya mengubah shell untuk Amazon Linux saya WorkSpace dan sekarang saya tidak dapat menyediakan sesi PCoIP

Untuk mengganti shell default untuk Linux WorkSpaces, lihatGanti shell default untuk Amazon Linux WorkSpaces.

Linux Amazon saya WorkSpaces tidak akan mulai

Mulai 20 Juli 2020, Amazon Linux WorkSpaces akan menggunakan sertifikat lisensi baru. Sertifikat baru ini kompatibel hanya dengan versi 2.14.1.1, 2.14.7, 2.14.9, dan 20.10.6 atau yang lebih baru dari agen PCoIP.

Jika Anda menggunakan versi yang tidak didukung dari agen PCoIP, Anda mesti meningkatkannya ke versi terbaru (20.10.6), yang memiliki perbaikan terbaru dan peningkatan performa yang kompatibel dengan sertifikat baru. Jika Anda tidak melakukan upgrade ini pada 20 Juli, penyediaan sesi untuk Linux Anda WorkSpaces akan gagal dan pengguna akhir Anda tidak akan dapat terhubung ke mereka. WorkSpaces

Untuk meningkatkan agen PCoIP Anda ke versi terbaru

1. Buka WorkSpaces konsol di https://console.aws.amazon.com/workspaces/.
2. Di panel navigasi, pilih WorkSpaces.
3. Pilih Linux Anda WorkSpace, dan reboot dengan memilih Actions, Reboot WorkSpaces. Jika WorkSpace statusnya`STOPPED`, Anda harus memilih Tindakan, Mulai WorkSpaces dulu dan tunggu sampai statusnya `AVAILABLE` sebelum Anda dapat mem-boot ulang.
4. WorkSpace Setelah Anda reboot dan statusnya`AVAILABLE`, kami sarankan Anda mengubah status WorkSpace ke `ADMIN_MAINTENANCE` saat Anda melakukan peningkatan ini. Setelah selesai, ubah status WorkSpace ke`AVAILABLE`. Untuk informasi selengkapnya mengenai mode `ADMIN_MAINTENANCE`, lihat Pemeliharaan Manual.

   Untuk mengubah status a WorkSpace ke`ADMIN_MAINTENANCE`, lakukan hal berikut:

a. Pilih WorkSpace dan pilih Tindakan, Ubah WorkSpace.

b. Pilih Modifikasi Status.

c. Untuk Keadaan yang Diinginkan, pilih ADMIN_MAINTENANCE.

d. Pilih Ubah.

5. Connect ke Linux Anda WorkSpace melalui SSH. Untuk informasi selengkapnya, lihat Aktifkan koneksi SSH untuk Linux Anda WorkSpaces.

6. Untuk memperbarui agen PCoIP, jalankan perintah berikut:

```
sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
```

7. Untuk memverifikasi versi agen dan untuk mengonfirmasi bahwa pembaruan berhasil, jalankan perintah berikut:

```
rpm -q pcoip-agent-standard
```

Perintah verifikasi harus menghasilkan beberapa hal sebagai berikut:

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. Putuskan sambungan dari WorkSpace dan reboot lagi.

9. Jika Anda menyetel status WorkSpace ke `ADMIN_MAINTENANCE` inStep 4, ulangi Step 4 dan setel Status yang Dimaksudkan ke`AVAILABLE`.

Jika Linux Anda WorkSpace masih gagal untuk memulai setelah Anda meng-upgrade agen PCoIP, hubungi Support AWS .

Peluncuran WorkSpaces di direktori saya yang terhubung sering gagal

Verifikasi bahwa dua server DNS atau pengontrol domain di direktori lokal Anda dapat diakses dari masing-masing subnet yang Anda tentukan saat terhubung ke direktori Anda. Anda dapat memverifikasi konektivitas ini dengan meluncurkan instans Amazon EC2 di setiap subnet dan bergabung dengan instans ke direktori Anda menggunakan alamat IP dari dua server DNS.

Peluncuran WorkSpaces gagal dengan kesalahan internal

Periksa apakah subnet Anda dikonfigurasi untuk secara otomatis menetapkan alamat IPv6 ke instans yang diluncurkan di subnet. Untuk memeriksa pengaturan ini, buka konsol Amazon VPC, pilih subnet Anda, dan pilih Tindakan Subnet, Ubah pengaturan IP tugas otomatis. Jika pengaturan ini diaktifkan, Anda tidak dapat meluncurkan WorkSpaces menggunakan bundel Kinerja atau Grafik. Sebaliknya, nonaktifkan pengaturan ini dan tentukan alamat IPv6 secara manual saat Anda meluncurkan instans Anda.

Ketika saya mencoba untuk mendaftar direktori, pendaftaran gagal dan meninggalkan direktori dalam keadaan KESALAHAN

Masalah ini dapat terjadi jika Anda mencoba mendaftarkan direktori Microsoft AD AWS Terkelola yang telah dikonfigurasi untuk replikasi Multi-wilayah. Meskipun direktori di Wilayah utama dapat berhasil didaftarkan untuk digunakan dengan Amazon WorkSpaces, mencoba mendaftarkan direktori di Wilayah yang direplikasi gagal. Replikasi Multi-Wilayah dengan AWS Microsoft AD Terkelola tidak didukung untuk digunakan dengan Amazon WorkSpaces dalam Wilayah yang direplikasi.

Pengguna saya tidak dapat terhubung ke Windows WorkSpace dengan spanduk masuk interaktif

Jika pesan masuk interaktif telah diterapkan untuk menampilkan spanduk masuk, ini mencegah pengguna untuk dapat mengakses Windows mereka. WorkSpaces Pengaturan Kebijakan Grup pesan masuk interaktif saat ini tidak didukung oleh WorkSpaces. Pindahkan WorkSpaces ke unit organisasi (OU) di mana Kebijakan Interactive logon: Message text for users attempting to log on Grup tidak diterapkan.

Pengguna saya tidak dapat terhubung ke Windows WorkSpace

Pengguna saya menerima kesalahan berikut ketika mereka mencoba untuk terhubung ke Windows mereka WorkSpaces:

```
"An error occurred while launching your WorkSpace. Please try again."
```

Kesalahan ini sering terjadi ketika tidak WorkSpace dapat memuat desktop Windows menggunakan PCoIP. Periksa hal-hal berikut:

- Pesan ini muncul jika Agen Standar PCoIP untuk Windows layanan tidak berjalan. Hubungkan menggunakan RDP untuk memverifikasi bahwa layanan berjalan, yang diatur untuk memulai secara otomatis, dan dapat berkomunikasi melalui antarmuka manajemen (eth0).

- Jika agen PCoIP dihapus, reboot melalui WorkSpaces konsol Amazon untuk WorkSpace menginstalnya kembali secara otomatis.

- Anda mungkin juga menerima kesalahan ini pada WorkSpaces klien Amazon setelah penundaan yang lama jika grup WorkSpaces keamanan dimodifikasi untuk membatasi lalu lintas keluar. Membatasi lalu lintas keluar mencegah Windows berkomunikasi dengan pengontrol direktori Anda untuk masuk. Verifikasi bahwa grup keamanan Anda memungkinkan Anda WorkSpaces untuk berkomunikasi dengan pengontrol direktori Anda pada semua port yang diperlukan melalui antarmuka jaringan utama.

Penyebab lain dari kesalahan ini terkait dengan Kebijakan Grup Penetapan Hak Pengguna. Jika kebijakan grup berikut tidak dikonfigurasi dengan benar, ini mencegah pengguna untuk dapat mengakses Windows mereka WorkSpaces:

Konfigurasi Komputer\ Pengaturan Windows\ Pengaturan Keamanan\ Kebijakan Lokal\ Penetapan Hak Pengguna

- Kebijakan yang salah:

  Kebijakan: Akses komputer ini dari jaringan

  Pengaturan: *Nama Domain*\Domain komputer

  Memenangkan GPO: Mengizinkan Akses File
- Kebijakan yang benar:

  Kebijakan: Akses komputer ini dari jaringan

  Pengaturan: *Nama Domain*\Pengguna Domain

  Memenangkan GPO: Mengizinkan Akses File

> **Note**
>
> Pengaturan kebijakan ini harus diterapkan untuk Pengguna Domain sebagai ganti Komputer Domain.

Untuk informasi selengkapnya, lihat Akses komputer ini dari jaringan - pengaturan kebijakan keamanan dan Mengonfigurasi pengaturan kebijakan keamanan dalam dokumentasi Microsoft Windows.

Pengguna saya mengalami masalah ketika mereka mencoba masuk WorkSpaces dari Akses WorkSpaces Web

Amazon WorkSpaces mengandalkan konfigurasi layar masuk tertentu untuk memungkinkan pengguna berhasil masuk dari klien Akses Web mereka.

Untuk mengaktifkan pengguna Akses Web untuk masuk ke mereka WorkSpaces, Anda harus mengkonfigurasi pengaturan Kebijakan Grup dan tiga pengaturan Kebijakan Keamanan. Jika pengaturan ini tidak dikonfigurasi dengan benar, pengguna mungkin mengalami waktu masuk yang lama atau layar hitam ketika mereka mencoba masuk ke pengaturan mereka WorkSpaces. Untuk mengonfigurasi pengaturan ini, lihat Aktifkan dan konfigurasikan Amazon WorkSpaces Web Access.

> **Important**
>
> Mulai 1 Oktober 2020, pelanggan tidak akan lagi dapat menggunakan klien Amazon WorkSpaces Web Access untuk terhubung ke kustom Windows 7 WorkSpaces atau ke Windows 7 Bring Your Own License (BYOL) WorkSpaces.

WorkSpaces Klien Amazon menampilkan layar abu-abu “Memuat...” untuk sementara waktu sebelum kembali ke layar login. Tidak ada pesan kesalahan lain yang muncul.

Perilaku ini biasanya menunjukkan bahwa WorkSpaces klien dapat mengautentikasi melalui port 443, tetapi tidak dapat membuat koneksi streaming melalui port 4172 (PCoIP) atau port 4195 (WSP). Situasi ini bisa terjadi ketika Prasyarat jaringan tidak terpenuhi. Masalah pada sisi klien sering menyebabkan jaringan cek di klien gagal. Untuk melihat pemeriksaan

kondisi mana yang gagal, pilih ikon pemeriksaan jaringan (biasanya segitiga merah dengan tanda seru di sudut kanan bawah layar masuk untuk klien 2.0+ atau ikon jaringan

di sudut kanan atas klie 3.0+).

> **Note**
>
> Penyebab paling umum dari masalah ini adalah firewall sisi klien atau proxy mencegah akses melalui port 4172 atau 4195 (TCP dan UDP). Jika pemeriksaan kondisi ini gagal, periksa pengaturan firewall lokal Anda.

Jika pemeriksaan jaringan lolos, mungkin ada masalah dengan konfigurasi jaringan WorkSpace. Sebagai contoh, aturan Windows Firewall mungkin memblokir port UDP 4172 atau 4195 pada antarmuka manajemen. Connect ke WorkSpace menggunakan klien Remote Desktop Protocol (RDP) untuk memverifikasi bahwa WorkSpace memenuhi persyaratan port yang diperlukan.

Pengguna saya menerima pesan "WorkSpace Status: Tidak sehat. Kami tidak dapat menghubungkan Anda dengan Anda WorkSpace. Coba lagi dalam beberapa menit."

Kesalahan ini biasanya menunjukkan SkyLightWorkSpacesConfigService layanan tidak menanggapi pemeriksaan kesehatan.

Jika Anda baru saja me-reboot atau memulai WorkSpace, tunggu beberapa menit, lalu coba lagi.

Jika WorkSpace telah berjalan selama beberapa waktu dan Anda masih melihat kesalahan ini, sambungkan menggunakan RDP untuk memverifikasi bahwa layanan: SkyLightWorkSpacesConfigService

- Menjalankan.
- Diatur untuk memulai secara otomatis.
- Dapat berkomunikasi melalui antarmuka manajemen (eth0).
- Tidak diblokir oleh perangkat lunak antivirus pihak ketiga.

Pengguna saya menerima pesan “Perangkat ini tidak diizinkan untuk mengakses WorkSpace. Hubungi administrator Amazon WorkDocs Anda untuk bantuan."

Kesalahan ini menunjukkan bahwa grup kontrol akses IP dikonfigurasi pada WorkSpace direktori, tetapi alamat IP klien tidak diizinkan terdaftar.

Periksa pengaturan pada direktori Anda. Konfirmasikan bahwa alamat IP publik yang terhubung pengguna memungkinkan akses ke WorkSpace.

Pengguna saya menerima pesan "Tidak ada jaringan. Hubungan jaringan hilang. Periksa hubungan jaringan Anda atau hubungi administrator Anda untuk mendapatkan bantuan." saat mencoba terhubung ke WSP WorkSpace

Jika kesalahan ini terjadi dan pengguna Anda tidak memiliki masalah konektivitas, pastikan bahwa port 4195 terbuka pada firewall jaringan Anda. Untuk WorkSpaces menggunakan WorkSpaces Streaming Protocol (WSP), port yang digunakan untuk streaming sesi klien diubah dari 4172 menjadi 4195.

WorkSpaces Klien memberi pengguna saya kesalahan jaringan, tetapi mereka dapat menggunakan aplikasi lain yang mendukung jaringan di perangkat mereka

Aplikasi WorkSpaces klien mengandalkan akses ke sumber daya di AWS Cloud, dan memerlukan koneksi yang menyediakan setidaknya 1 Mbps bandwidth unduhan. Jika perangkat memiliki koneksi intermiten ke jaringan, aplikasi WorkSpaces klien mungkin melaporkan masalah dengan jaringan.

WorkSpaces memberlakukan penggunaan sertifikat digital yang dikeluarkan oleh Amazon Trust Services, per Mei 2018. Amazon Trust Services sudah menjadi Root CA tepercaya pada sistem operasi yang didukung oleh WorkSpaces. Jika daftar Root CA untuk sistem operasi tidak mutakhir, perangkat tidak dapat terhubung WorkSpaces dan klien memberikan kesalahan jaringan.

Untuk mengenali masalah hubungan karena kegagalan sertifikat

- Klien nol PCoIP - Pesan kesalahan berikut ditampilkan.

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- Klien lain — Pemeriksaan kondisi gagal dengan segitiga peringatan merah untuk Internet.

Untuk mengatasi kegagalan sertifikat

- Aplikasi klien Windows
- Klien nol PCoIP
- Aplikasi klien lain

Aplikasi klien Windows

Gunakan salah satu solusi berikut untuk kegagalan sertifikat.

Solusi 1: Perbarui aplikasi klien

Unduh dan instal aplikasi klien Windows terbaru dari https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east Selama instalasi, aplikasi klien memastikan bahwa sistem operasi Anda mempercayai sertifikat yang dikeluarkan oleh Amazon Trust Services.

Solusi 2: Tambahkan Amazon Trust Services ke daftar Root CA lokal

1. Buka https://www.amazontrust.com/repository/.
2. Unduh sertifikat Starfield dalam format DER (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92).
3. Buka konsol manajemen Microsoft. (Dari Prompt Perintah, jalankan mmc.)
4. Pilih File, Tambahkan/Hapus Snap-in, Sertifikat, Tambahkan.
5. Pada halaman Sertifikat snap-in, pilih Akun komputer dan pilih Selanjutnya. Jaga default,Komputer lokal. Pilih Selesai. Pilih OK.
6. Perluas Sertifikat (komputer lokal) dan pili hOtoritas Sertifikasi Root Terpercaya. Pilih Tindakan, Semua Tugas, Impor.
7. Ikuti wizard untuk mengimpor sertifikat yang Anda unduh.
8. Keluar dan mulai ulang aplikasi WorkSpaces klien.

Solusi 3: Deploy Amazon Trust Services sebagai CA terpercaya menggunakan Kebijakan Grup

Tambahkan sertifikat Starfield ke Root CA tepercaya untuk domain yang menggunakan Kebijakan Grup. Untuk informasi selengkapnya, lihat Gunakan kebijakan untuk mendistribusikan sertifikat.

Klien nol PCoIP

Untuk terhubung langsung ke firmware WorkSpace menggunakan versi 6.0 atau yang lebih baru, unduh dan instal sertifikat yang dikeluarkan oleh Amazon Trust Services.

Untuk menambahkan Amazon Trust Services sebagai Root CA terpercaya

1. Buka https://certs.secureserver.net/repository/.
2. Unduh sertifikat di bawah Rantai Sertifikat Starfield dengan thumbprint 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58.
3. Unggah sertifikat ke CDN. Untuk informasi selengkapnya, lihat Mengunggah Sertifikat dalam dokumentasi Teradici.

Aplikasi klien lain

Tambahkan sertifikat Starfield (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) dari Amazon Trust Services. Untuk informasi selengkapnya tentang cara menambahkan Root CA, lihat dokumentasi berikut:

- Android: Tambah & hapus sertifikat
- Chrome OS: Kelola sertifikat klien di perangkat Chrome
- macOS dan iOS: Menginstal sertifikat Root CA pada perangkat tes Anda

WorkSpace Pengguna saya melihat pesan galat berikut: “Perangkat tidak dapat terhubung ke layanan pendaftaran. Periksa pengaturan jaringan Anda."

Ketika terjadi kegagalan layanan pendaftaran, WorkSpace pengguna Anda mungkin melihat pesan galat berikut di halaman Pemeriksaan Kesehatan Sambungan: “Perangkat Anda tidak dapat terhubung ke layanan WorkSpaces Pendaftaran. Anda tidak akan dapat mendaftarkan perangkat Anda WorkSpaces. Silakan periksa pengaturan jaringan Anda."

Kesalahan ini terjadi ketika aplikasi WorkSpaces klien tidak dapat mencapai layanan pendaftaran. Biasanya, ini terjadi ketika WorkSpaces direktori telah dihapus. Untuk mengatasi kesalahan ini, pastikan kode registrasi valid dan sesuai dengan direktori yang sedang berjalan di AWS Cloud.

Pengguna klien nol PCoIP menerima kesalahan "Sertifikat yang disediakan tidak valid karena timestamp"

Jika Network Time Protocol (NTP) tidak diaktifkan di Teradici, pengguna klien nol PCoIP mungkin menerima kesalahan kegagalan sertifikat. Untuk mengatur NTP, lihat Siapkan klien nol PCoIP untuk WorkSpaces.

Printer USB dan periferal USB lainnya tidak bekerja untuk klien nol PCoIP

Dimulai dengan versi 20.10.4 dari agen PCoIP, Amazon WorkSpaces menonaktifkan pengalihan USB secara default melalui registri Windows. Pengaturan registri ini memengaruhi perilaku periferal USB saat pengguna Anda menggunakan perangkat klien nol PCoIP untuk terhubung ke perangkat mereka. WorkSpaces

Jika Anda WorkSpaces menggunakan agen PCoIP versi 20.10.4 atau yang lebih baru, perangkat periferal USB tidak akan berfungsi dengan perangkat klien nol PCoIP hingga Anda mengaktifkan pengalihan USB.

> **Note**
>
> Jika Anda menggunakan driver printer virtual 32-bit, Anda juga harus memperbarui driver tersebut ke versi 64-bit.

Untuk mengaktifkan pengalihan USB untuk perangkat klien nol PCoIP

Kami menyarankan Anda untuk mendorong perubahan registri ini ke Kebijakan Grup WorkSpaces melalui Anda. Untuk informasi selengkapnya, lihat, Mengonfigurasi agen dan Pengaturan yang dapat dikonfigurasi dalam dokumentasi Teradici.

1. Tetapkan nilai kunci registri berikut ke 1 (diaktifkan):

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Kebijakan\ Teradici\ PCoIP\ pcoip_admin

   KeyName = pcoip.enable_usb

KeyType = DWORD

KeyValue = 1

2. Tetapkan nilai kunci registri berikut ke 1 (diaktifkan):

   KeyPath = HKEY_LOCAL_MACHINE\ PERANGKAT LUNAK\ Kebijakan\ Teradici\ PCoIP\ pcoip_admin_defaults

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1

3. Jika Anda belum melakukannya, keluar dari WorkSpace, lalu masuk kembali. Perangkat USB Anda seharusnya sekarang bekerja.

Pengguna saya melewatkan pembaruan aplikasi klien Windows atau macOS mereka dan tidak diminta untuk menginstal versi terbaru

Ketika pengguna melewatkan pembaruan ke aplikasi klien Amazon WorkSpaces Windows, kunci SkipThisVersionregistri akan disetel, dan mereka tidak lagi diminta untuk memperbarui klien mereka ketika versi baru klien dirilis. Untuk memperbarui ke versi terbaru, Anda dapat mengedit registri seperti yang dijelaskan dalam Perbarui Aplikasi Klien WorkSpaces Windows ke Versi yang Lebih Baru di Panduan WorkSpaces Pengguna Amazon. Anda juga dapat menjalankan PowerShell perintah berikut:

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

Ketika pengguna melewatkan pembaruan ke aplikasi klien Amazon WorkSpaces macOS, `SUSkippedVersion` preferensi akan ditetapkan, dan mereka tidak lagi diminta untuk memperbarui klien mereka ketika versi baru klien dirilis. Untuk memperbarui ke versi terbaru, Anda dapat mengatur ulang preferensi ini seperti yang dijelaskan dalam Perbarui Aplikasi Klien WorkSpaces macOS ke Versi yang Lebih Baru di Panduan Pengguna Amazon WorkSpaces .

Pengguna saya tidak dapat memasang aplikasi klien Android di Chromebook mereka

Versi 2.4.13 adalah rilis final dari aplikasi klien Amazon WorkSpaces Chromebook. Karena Google menghapus dukungan untuk Aplikasi Chrome secara bertahap, tidak akan ada pembaruan lebih lanjut untuk aplikasi klien WorkSpaces Chromebook, dan penggunaannya tidak didukung.

Untuk Chromebook yang mendukung penginstalan aplikasi Android, sebaiknya gunakan aplikasi klien WorkSpaces Android sebagai gantinya.

Dalam beberapa kasus, Anda mungkin perlu mengaktifkan Chromebook pengguna untuk menginstal aplikasi Android. Untuk informasi selengkapnya, lihat Atur Android untuk Chromebook.

Pengguna saya tidak menerima email undangan atau email pengaturan ulang kata sandi

Pengguna tidak secara otomatis menerima email selamat datang atau pengaturan ulang kata sandi untuk email WorkSpaces yang dibuat menggunakan AD Connector atau domain tepercaya. Email undangan juga tidak dikirim secara otomatis jika pengguna sudah ada di Direktori Aktif.

Untuk mengirim email selamat datang secara manual kepada pengguna ini, lihat Kirim email undangan.

Untuk mengatur ulang kata sandi pengguna, lihat Siapkan Alat Administrasi Direktori Aktif untuk WorkSpaces.

Pengguna saya tidak melihat opsi Lupa kata sandi? pada layar masuk klien

Jika Anda menggunakan AD Connector atau domain tepercaya, pengguna Anda tidak akan dapat mengatur ulang kata sandi mereka sendiri. (Lupa kata sandi? pilihan pada layar login aplikasi WorkSpaces klien tidak akan tersedia.) Untuk informasi tentang cara mengatur ulang kata sandi pengguna, lihat Siapkan Alat Administrasi Direktori Aktif untuk WorkSpaces.

Saya menerima pesan “Administrator sistem telah menetapkan kebijakan untuk mencegah instalasi ini” ketika saya mencoba menginstal aplikasi pada Windows WorkSpace

Anda dapat mengatasi masalah ini dengan memodifikasi pengaturan Kebijakan Grup Penginstal Windows. Untuk menerapkan kebijakan ini ke beberapa WorkSpaces di direktori Anda, terapkan

setelan ini ke objek Kebijakan Grup yang ditautkan ke unit WorkSpaces organisasi (OU) dari instans EC2 yang bergabung dengan domain. Jika Anda menggunakan AD Connector, Anda dapat membuat perubahan ini dari pengendali domain. Untuk informasi selengkapnya tentang menggunakan alat administrasi Direktori Aktif untuk bekerja dengan objek Kebijakan Grup, lihat Menginstal alat administrasi direktori aktif di Panduan Administrasi AWS Directory Service .

Prosedur berikut menunjukkan cara mengkonfigurasi pengaturan Windows Installer untuk objek Kebijakan WorkSpaces Grup.

1. Pastikan bahwa template administratif Kebijakan WorkSpaces Grup terbaru diinstal di domain Anda.
2. Buka alat Manajemen Kebijakan Grup pada WorkSpace klien Windows Anda dan arahkan ke dan pilih objek Kebijakan WorkSpaces Grup untuk akun WorkSpaces mesin Anda. Dari menu utama, pilih Tindakan, Edit.
3. Di Editor Manajemen Kebijakan Grup, pilih Konfigurasi komputer, Kebijakan, Templat administratif, Templat Administratif Klasik, Komponen Windows, Pemasang Windows.
4. Buka pengaturan Matikan Penginstal Windows.
5. Pada kotak dialog Matikan Penginstal Windows, ubah Tidak Terkonfigurasi menjadi Diaktifkan, lalu atur Nonaktifkan Penginstal Windows menjadi Tidak pernah.
6. Pilih OKE.
7. Untuk menerapkan perubahan kebijakan grup, lakukan salah satu hal berikut:
   - Reboot WorkSpace (di WorkSpaces konsol, pilih WorkSpace, lalu pilih Tindakan, Reboot WorkSpaces).
   - Dari prompt perintah administratif, masukkan gpupdate /force.

Tidak ada WorkSpaces di direktori saya yang dapat terhubung ke internet

WorkSpaces tidak dapat berkomunikasi dengan internet secara default. Anda harus secara eksplisit menyediakan akses internet. Untuk informasi selengkapnya, lihat Menyediakan akses internet dari Anda WorkSpace.

Saya WorkSpace telah kehilangan akses internetnya

Jika Anda WorkSpace telah kehilangan akses ke internet dan Anda tidak dapat terhubung ke WorkSpace dengan menggunakan RDP, masalah ini mungkin disebabkan oleh hilangnya alamat

IP publik untuk. WorkSpace Jika Anda telah mengaktifkan penetapan otomatis alamat IP Elastis di tingkat direktori, alamat IP Elastis (dari kumpulan yang disediakan Amazon) ditetapkan untuk Anda WorkSpace saat diluncurkan. Namun, jika Anda mengaitkan alamat IP Elastis yang Anda miliki ke WorkSpace, dan kemudian Anda kemudian memisahkan alamat IP Elastis itu dari WorkSpace, alamat IP publiknya WorkSpace kehilangan, dan itu tidak secara otomatis mendapatkan yang baru dari kumpulan yang disediakan Amazon.

Untuk mengaitkan alamat IP publik baru dari kumpulan yang disediakan Amazon dengan WorkSpace, Anda harus membangun kembali. WorkSpace Jika Anda tidak ingin membangun kembali WorkSpace, Anda harus mengaitkan alamat IP Elastis lain yang Anda miliki ke alamat IP Elastic. WorkSpace

Kami menyarankan Anda untuk tidak memodifikasi elastic network interface WorkSpace setelah diluncurkan. WorkSpace Setelah alamat IP Elastis ditetapkan ke a WorkSpace, alamat IP publik yang sama WorkSpace mempertahankan alamat IP publik yang sama (kecuali jika dibangun kembali, dalam hal ini mendapat alamat IP publik baru). WorkSpace

Saya menerima kesalahan "DNS tidak tersedia" ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan kesalahan yang serupa dengan hal berikut ini saat menghubungkan ke direktori on-premise Anda.

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connector harus dapat berkomunikasi dengan server DNS on-premise Anda melalui TCP dan UDP melewati port 53. Verifikasi bahwa grup keamanan dan firewall on-premise mengizinkan komunikasi TCP dan UDP melewati port ini.

Saya menerima kesalahan "Masalah hubungan terdeteksi" ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan kesalahan yang serupa dengan hal berikut ini saat menghubungkan ke direktori on-premise Anda.

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
```

```
Please ensure that the listed ports are available and retry the operation.
```

AD Connector harus dapat berkomunikasi dengan pengendali domain on-premise Anda melalui TCP dan UDP melewati port-port berikut. Verifikasi bahwa grup keamanan dan firewall on-premise mengizinkan komunikasi TCP dan UDP melewati port-port ini:

- 88 (Kerberos)
- 389 (LDAP)

Saya menerima kesalahan "catatan SRV" ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan kesalahan yang serupa dengan satu atau beberapa poin berikut ini saat menghubungkan ke direktori on-premise Anda.

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

AD Connector perlu memperoleh catatan SRV `_ldap._tcp.`*`dns-domain-name`* dan `_kerberos._tcp.`*`dns-domain-name`* saat menghubungkan ke direktori Anda. Anda akan mendapatkan error ini jika layanan tidak dapat memperoleh catatan ini dari server DNS yang Anda tentukan saat menghubungkan ke direktori Anda. Pastikan bahwa server DNS berisi data SRV ini. Untuk informasi selengkapnya, lihat Catatan Sumber Daya SRV di Microsoft TechNet.

WorkSpace Jendela saya tertidur ketika dibiarkan menganggur

Untuk mengatasi masalah ini, sambungkan ke WorkSpace dan ubah rencana daya ke Kinerja tinggi dengan menggunakan prosedur berikut:

1. Dari WorkSpace, buka Control Panel, lalu pilih Hardware atau pilih Hardware and Sound (namanya mungkin berbeda, tergantung pada versi Windows Anda).
2. Di bawah Opsi Daya, pilih Pilih paket daya.
3. Pada panel Pilih atau sesuaikan paket daya, pilih rencana daya Performa tinggi, lalu pilih Ubah pengaturan rencana.
   - Jika opsi untuk memilih rencana daya Performa tinggi dinonaktifkan, pilih Ubah setelan yang saat ini tidak tersedia, lalu pilih rencana daya Performa tinggi.

- Jika rencana Performa tinggi tidak terlihat, pilih panah di sebelah kanan dari Tampilkan rencana tambahan untuk menampilkannya, atau pilih Buat rencana daya di navigasi kiri, pilih Performa tinggi, beri rencana daya sebuah nama, lalu pilih Selanjutnya.

4. Pada halaman Ubah pengaturan untuk rencana: Performa tinggi, pastikan Matikan tampilan dan (jika tersedia) Aktifkan sleep pada komputer diatur ke Tidak pernah.
5. Jika Anda membuat perubahan pada rencana performa tinggi, pilih Simpan perubahan (atau pilih Buat jika Anda membuat rencana baru).

Jika langkah-langkah sebelumnya tidak menyelesaikan masalah, lakukan hal berikut:

1. Dari WorkSpace, buka Control Panel, lalu pilih Hardware atau pilih Hardware and Sound (namanya mungkin berbeda, tergantung pada versi Windows Anda).
2. Di bawah Opsi Daya, pilih Pilih paket daya.
3. Pada panel Pilih atau sesuaikan rencana daya, pilih Ubah pengaturan rencana link ke kanan dari Performa tinggi, lalu pilih tautan Ubah setelan daya tingkat lanjut.
4. Di kotak dialog Opsi Daya, dalam daftar pengaturan, pilih tanda tambah di sebelah kiri dari Hard Disk untuk menampilkan pengaturan yang relevan.
5. Verifikasi bahwa Matikan hard disk setelah nilai agar Terpasang lebih besar dari nilai untuk Baterai (nilai default adalah 20 menit).
6. Pilih tanda tambah di sebelah kiri PCI Express, dan lakukan hal yang sama untuk Link State Power Management.
7. Verifikasi bahwa pengaturan Link State Power Management Mati.
8. Pilih OKE (atau Terapkan jika Anda mengubah pengaturan apa pun) untuk menutup kotak dialog.
9. Pada panel Ubah setelan untuk rencana, jika Anda mengubah pengaturan apa pun, pilih Simpan perubahan.

Salah satu dari saya WorkSpaces memiliki keadaan **UNHEALTHY**

WorkSpaces Layanan secara berkala mengirimkan permintaan status ke a WorkSpace. A WorkSpace ditandai `UNHEALTHY` ketika gagal menanggapi permintaan ini. Penyebab umum untuk masalah ini adalah:

- Aplikasi pada WorkSpace memblokir port jaringan, yang mencegah WorkSpace dari menanggapi permintaan status.

- Pemanfaatan CPU yang tinggi mencegah WorkSpace dari menanggapi permintaan status secara tepat waktu.
- Nama komputer WorkSpace telah diubah. Ini mencegah saluran aman dibuat antara WorkSpaces dan WorkSpace.

Anda dapat mencoba untuk memperbaiki situasi menggunakan metode berikut:

- Reboot WorkSpace dari WorkSpaces konsol.
- Connect ke yang tidak sehat WorkSpace menggunakan prosedur berikut, yang harus digunakan hanya untuk tujuan pemecahan masalah:

  1. Connect ke operasional WorkSpace di direktori yang sama dengan yang tidak sehat WorkSpace.
  2. Dari operasional WorkSpace, gunakan Remote Desktop Protocol (RDP) untuk terhubung ke yang tidak sehat WorkSpace menggunakan alamat IP yang tidak sehat. WorkSpace Tergantung pada sejauh mana masalahnya, Anda mungkin tidak dapat terhubung ke yang tidak sehat WorkSpace.
  3. Pada yang tidak sehat WorkSpace, konfirmasikan bahwa persyaratan port minimum terpenuhi.
- Pastikan SkyLightWorkSpacesConfigService layanan dapat merespon pemeriksaan kesehatan. Untuk memecahkan masalah ini, lihat Pengguna saya menerima pesan "WorkSpace Status: Tidak sehat. Kami tidak dapat menghubungkan Anda dengan Anda WorkSpace. Coba lagi dalam beberapa menit.".
- Membangun kembali WorkSpace dari WorkSpaces konsol. Karena membangun kembali WorkSpace dapat berpotensi menyebabkan hilangnya data, opsi ini harus digunakan hanya jika semua upaya lain untuk memperbaiki masalah tidak berhasil.

Saya WorkSpace tiba-tiba mogok atau reboot

Jika WorkSpace dikonfigurasi untuk PCoIP berulang kali mogok atau reboot dan log kesalahan atau crash dump mengarah ke masalah dengan atau`spacedeskHookUmode.dll`, `spacedeskHookKmode.sys` atau jika Anda menerima pesan galat berikut, Anda mungkin perlu menonaktifkan Akses Web ke: WorkSpace

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - Langkah-langkah pemecahan masalah ini tidak berlaku untuk WorkSpaces yang dikonfigurasi untuk WorkSpaces Streaming Protocol (WSP). Mereka hanya berlaku untuk WorkSpaces yang dikonfigurasi untuk PCoIP.
> - Anda harus menonaktifkan akses Web hanya jika Anda tidak mengizinkan pengguna Anda untuk menggunakan akses Web.

Untuk menonaktifkan Akses Web ke WorkSpace, Anda harus menonaktifkan Akses Web di WorkSpaces direktori dan reboot WorkSpace.

Nama pengguna yang sama memiliki lebih dari satu WorkSpace, tetapi pengguna hanya dapat masuk ke salah satu WorkSpaces

Jika Anda menghapus pengguna di Active Directory (AD) tanpa terlebih dahulu menghapusnya WorkSpace dan kemudian Anda menambahkan pengguna kembali ke Active Directory dan membuat yang baru WorkSpace untuk pengguna itu, nama pengguna yang sama sekarang akan memiliki dua WorkSpaces di direktori yang sama. Namun, jika pengguna mencoba untuk terhubung ke aslinya WorkSpace, mereka akan menerima kesalahan berikut:

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

Selain itu, pencarian nama pengguna di WorkSpaces konsol Amazon hanya mengembalikan yang baru WorkSpace, meskipun keduanya WorkSpaces masih ada. (Anda dapat menemukan yang asli WorkSpace dengan mencari WorkSpace ID alih-alih nama pengguna.)

Perilaku ini juga dapat terjadi jika Anda mengganti nama pengguna di Active Directory tanpa terlebih dahulu menghapusnya. WorkSpace Jika Anda kemudian mengubah nama pengguna mereka kembali ke nama pengguna asli dan membuat yang baru WorkSpace untuk pengguna, nama pengguna yang sama akan memiliki dua WorkSpaces di direktori.

Masalah ini terjadi karena Direktori Aktif menggunakan pengguna keamanan identifier (SID), bukan nama pengguna, untuk secara unik mengidentifikasi pengguna. Ketika pengguna dihapus dan dibuat

ulang di Direktori Aktif, pengguna ditetapkan SID baru, bahkan jika nama pengguna mereka tetap sama. Selama mencari nama pengguna, WorkSpaces konsol Amazon menggunakan SID untuk mencari Active Directory untuk kecocokan. WorkSpaces Klien Amazon juga menggunakan SID untuk mengidentifikasi pengguna saat mereka terhubung WorkSpaces.

Untuk menyelesaikan masalah ini, coba hal berikut:

- Jika masalah ini terjadi karena pengguna telah dihapus dan dibuat ulang di Direktori Aktif, Anda mungkin dapat memulihkan objek pengguna asli yang dihapus jika Anda telah mengaktifkan Fitur keranjang sampah di Direktori Aktif. Jika Anda dapat memulihkan objek pengguna asli, pastikan pengguna dapat terhubung ke aslinya WorkSpace. Jika bisa, Anda dapat menghapus yang baru WorkSpace setelah mencadangkan dan mentransfer data pengguna secara manual dari yang baru WorkSpace ke yang asli WorkSpace (jika diperlukan).
- Jika Anda tidak dapat memulihkan objek pengguna asli, hapus asli pengguna WorkSpace. Pengguna harus dapat terhubung dan menggunakan yang baru WorkSpace sebagai gantinya. Pastikan untuk mencadangkan dan mentransfer data pengguna secara manual dari yang asli WorkSpace ke yang baru WorkSpace.

> **Warning**
>
> Menghapus a WorkSpace adalah tindakan permanen dan tidak dapat dibatalkan. Data WorkSpace pengguna tidak bertahan dan dihancurkan. Untuk bantuan dengan mencadangkan data pengguna, hubungi AWS Support.

Saya mengalami masalah dalam menggunakan Docker dengan Amazon WorkSpaces

Jendela WorkSpaces

Virtualisasi bersarang (termasuk penggunaan Docker) tidak didukung di Windows. WorkSpaces Untuk informasi selengkapnya, lihat Dokumentasi Docker.

Linux WorkSpaces

Untuk menggunakan Docker di Linux WorkSpaces, pastikan bahwa blok CIDR yang digunakan oleh Docker tidak tumpang tindih dengan blok CIDR yang digunakan dalam dua antarmuka jaringan elastis (ENI) yang terkait dengan. WorkSpace Jika Anda mengalami masalah dengan menggunakan Docker di Linux WorkSpaces, hubungi Docker untuk bantuan.

Saya menerima ThrottlingException kesalahan pada beberapa panggilan API saya

Rasio default yang diizinkan untuk panggilan WorkSpaces API adalah tingkat konstan dua panggilan API per detik, dengan tingkat “burst” maksimum yang diizinkan lima panggilan API per detik. Tabel berikut menunjukkan bagaimana batas burst rate bekerja untuk permintaan API.

Detik	Jumlah Permintaan dikirim	Permintaan net diperbolehkan	Detail
1	0	5	Selama detik pertama (kedua 1), lima permintaan diperbolehkan, hingga tingkat ledakan maksimum lima panggilan per detik.
2	2	5	Karena dua atau lebih sedikit panggilan dikeluarkan di kedua 1, kapasitas lonjakan lima panggilan masih tersedia.
3	5	5	Karena hanya dua panggilan yang dikeluarkan di kedua 2, kapasitas lonjakan lima panggilan masih tersedia.
4	2	2	Karena kapasitas lonjakan penuh digunakan di kedua 3, hanya tingkat konstan dua panggilan per detik tersedia.
5	3	2	Karena tidak ada kapasitas lonjakan yang tersisa, hanya dua panggilan yang diizinkan saat ini. Ini berarti bahwa salah satu dari tiga panggilan API dicekik. Panggilan yang throttled akan merespons setelah penundaan singkat.
6	0	1	Karena salah satu panggilan dari detik 5 sedang dicoba di detik 6, ada kapasitas untuk hanya satu panggilan tambahan di detik 6 karena batas tingkat konstan dua panggilan per detik.

Detik	Jumlah Permintaan dikirim	Permintaan net diperbolehkan	Detail
7	0	3	Sekarang bahwa ada tidak lagi setiap throttle API panggilan dalam antrean, batas tingkat terus meningkat, sampai batas tingkat ledakan lima panggilan.
8	0	5	Karena tidak ada panggilan yang dikeluarkan di detik 7, jumlah maksimum permintaan diperbolehkan.
9	0	5	Meskipun tidak ada panggilan yang dikeluarkan di kedua 8, batas tarif tidak meningkat di atas lima.

Saya WorkSpace terus terputus ketika saya membiarkannya berjalan di latar belakang

Untuk pengguna Mac, periksa untuk melihat apakah fitur Power Nap aktif. Jika menyala, matikan. Untuk mematikan Power Nap, buka terminal Anda dan jalankan perintah berikut:

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

Federasi SAFL 2.0 tidak berfungsi. Pengguna saya tidak berwenang untuk melakukan streaming WorkSpaces desktop mereka.

Ini mungkin terjadi karena kebijakan sebaris yang disematkan untuk peran IAM federasi SAMP 2.0 tidak menyertakan izin untuk melakukan streaming dari direktori Amazon Resource Name (ARN). Peran IAM diasumsikan oleh pengguna federasi yang mengakses direktori. WorkSpaces Edit izin peran untuk menyertakan direktori ARN dan memastikan bahwa pengguna WorkSpace memiliki di direktori. Untuk informasi selengkapnya, lihat Otentikasi SAMP 2.0 dan Pemecahan Masalah Federasi SAMP 2.0 dengan. AWS

Pengguna saya terputus dari WorkSpaces sesi mereka setiap 60 menit.

Jika Anda telah mengonfigurasi otentikasi SAMP 2.0 WorkSpaces, tergantung pada penyedia identitas (iDP), Anda mungkin perlu mengonfigurasi informasi yang diteruskan IDP sebagai atribut SAMP sebagai bagian dari respons otentikasi. AWS Ini termasuk mengkonfigurasi elemen Atribut dengan **`SessionDuration`** atribut yang disetel ke`https://aws.amazon.com/SAML/Attributes/SessionDuration`.

`SessionDuration`menentukan jumlah waktu maksimum bahwa sesi streaming federasi dapat tetap aktif untuk pengguna sebelum otentikasi ulang diperlukan. Meskipun `SessionDuration` merupakan atribut opsional, kami sarankan Anda memasukkannya ke dalam respons otentikasi SAMP. Jika Anda tidak menentukan atribut ini, durasi sesi default menjadi 60 menit.

Untuk mengatasi masalah ini, konfigurasikan IDP Anda untuk menyertakan `SessionDuration` nilai dalam respons otentikasi SAMP dan tetapkan nilainya sesuai kebutuhan. Untuk informasi selengkapnya, lihat Langkah 5: Membuat pernyataan untuk respons otentikasi SAMP.

Pengguna saya mendapatkan kesalahan URI pengalihan ketika mereka melakukan federasi menggunakan aliran yang dimulai oleh penyedia identitas SAMP 2.0 (iDP), atau instance tambahan dari aplikasi WorkSpaces klien dimulai setiap kali pengguna saya mencoba masuk dari klien setelah federasi ke iDP.

Kesalahan ini terjadi karena URL status relay yang tidak valid. Pastikan bahwa status relai dalam pengaturan federasi IDP Anda sudah benar, dan bahwa URL akses pengguna dan nama parameter status relai dikonfigurasi dengan benar untuk federasi iDP Anda di properti direktori. WorkSpaces Jika valid dan masalah masih berlanjut, hubungi AWS Support. Untuk informasi selengkapnya, lihat Menyiapkan SAMP.

Pengguna saya menerima pesan, “Ada yang tidak beres: Terjadi kesalahan saat meluncurkan WorkSpace" ketika mereka mencoba masuk ke aplikasi WorkSpaces klien setelah federasi ke iDP.

Tinjau pernyataan SAMP 2.0 untuk federasi Anda. Nilai NameID Subjek SAMP harus cocok dengan WorkSpaces nama pengguna, dan biasanya sama dengan atribut AccountName SAM untuk pengguna Active Directory. Selain itu, elemen Atribut yang memiliki `PrincipalTag:Email` atribut

yang disetel `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` harus cocok dengan alamat email WorkSpaces pengguna seperti yang didefinisikan dalam WorkSpaces direktori. Untuk informasi selengkapnya, lihat Menyiapkan SAMP.

Pengguna saya menerima pesan, “Tidak dapat memvalidasi tag” ketika mereka mencoba masuk ke aplikasi WorkSpaces klien setelah federasi ke iDP.

Tinjau nilai `PrincipalTag` atribut dalam pernyataan SAMP 2.0 untuk federasi Anda, seperti. `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` Nilai tag dapat mencakup kombinasi karakter`_ . : / = + - @`, huruf, angka, dan spasi.. Untuk informasi selengkapnya, lihat Aturan untuk menandai di IAM dan. AWS STS

Pengguna saya menerima pesan, “Klien dan server tidak dapat berkomunikasi, karena mereka tidak memiliki algoritma umum”.

Masalah ini dapat terjadi jika Anda tidak mengaktifkan TLS 1.2.

Mikrofon atau kamera web saya tidak berfungsi di Windows WorkSpaces.

Periksa pengaturan privasi Anda dengan membuka menu Start

- Mulai> Pengaturan > Privasi > Kamera
- Mulai> Pengaturan > Privasi > Mikrofon

Jika dimatikan, nyalakan.

Atau, WorkSpaces administrator dapat membuat Objek Kebijakan Grup (GPO) untuk mengaktifkan mikrofon dan atau webcam sesuai kebutuhan.

Pengguna saya tidak dapat masuk menggunakan otentikasi berbasis sertifikat dan diminta untuk kata sandi baik di WorkSpaces klien atau layar masuk Windows saat mereka terhubung ke sesi desktop mereka.

Otentikasi berbasis sertifikat tidak berhasil untuk sesi tersebut. Jika masalah berlanjut, kegagalan otentikasi berbasis sertifikat dapat menjadi hasil dari salah satu masalah berikut:

- Klien WorkSpaces atau tidak didukung. Otentikasi berbasis sertifikat didukung dengan bundel Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) menggunakan aplikasi klien Windows terbaru. WorkSpaces
- WorkSpaces Perlu di-boot ulang setelah mengaktifkan otentikasi berbasis sertifikat pada Direktori. WorkSpaces
- WorkSpaces tidak dapat berkomunikasi dengan AWS Private CA, atau AWS Private CA tidak mengeluarkan sertifikat. Periksa AWS CloudTrailuntuk menentukan apakah sertifikat dikeluarkan. Untuk informasi selengkapnya, lihat Kelola otentikasi berbasis sertifikat.
- Pengontrol domain tidak memiliki sertifikat pengontrol domain untuk logon kartu pintar, atau kedaluwarsa. Untuk informasi selengkapnya, lihat langkah 7, “Konfigurasikan pengontrol domain dengan sertifikat pengontrol domain untuk mengautentikasi pengguna kartu pintar” di. Prasyarat
- Sertifikat tidak dipercaya. Untuk informasi selengkapnya, lihat langkah 7, “Publikasikan CA ke Direktori Aktif” diPrasyarat. Jalankan `certutil -viewstore -enterprise NTAuth` pada pengontrol domain untuk mengonfirmasi bahwa CA diterbitkan.
- Ada sertifikat dalam cache, tetapi atribut telah berubah untuk pengguna yang telah membatalkan sertifikat. Kontak AWS Support untuk menghapus cache sebelum sertifikat kedaluwarsa (24 jam). Untuk informasi lebih lanjut, lihat AWS Support Pusat.
- userPrincipalName Format untuk atribut `UserPrincipalName` SAMP tidak diformat dengan benar atau tidak menyelesaikan ke domain aktual untuk pengguna. Untuk informasi lebih lanjut, lihat langkah 1 diPrasyarat.
- `ObjectSid`Atribut (opsional) dalam pernyataan SAMP Anda tidak cocok dengan pengenal keamanan Direktori Aktif (SID) untuk pengguna yang ditentukan dalam SAML_subject. `NameID` Konfirmasikan bahwa pemetaan atribut sudah benar di federasi SAMP Anda dan bahwa penyedia identitas SAMP Anda menyinkronkan atribut SID untuk pengguna Active Directory.
- Ada pengaturan Kebijakan Grup yang memodifikasi pengaturan Active Directory default untuk logon kartu pintar atau mengambil tindakan jika kartu pintar dihapus dari pembaca kartu pintar. Pengaturan ini dapat menyebabkan perilaku tak terduga tambahan daripada kesalahan yang tercantum di atas. Otentikasi berbasis sertifikat menyajikan kartu pintar virtual ke sistem operasi instance dan menghapusnya setelah logon selesai. Periksa pengaturan Kebijakan Grup Utama untuk kartu pintar dan pengaturan Kebijakan Grup kartu pintar tambahan dan kunci registri, termasuk perilaku penghapusan kartu pintar.
- Titik distribusi CRL untuk CA pribadi tidak online atau dapat diakses baik dari WorkSpaces atau pengontrol domain. Untuk informasi selengkapnya, lihat langkah 5 di Prasyarat.

- Untuk memeriksa apakah ada CA basi di domain atau hutan, jalankan `PKIVIEW.msc` di CA untuk memverifikasi. Jika ada CA basi, gunakan `PKIVIEW.msc` mmc untuk menghapusnya secara manual.
- Untuk memeriksa apakah replikasi Active Directory berfungsi dan tidak ada pengontrol domain basi di domain, jalankan. `repadmin /replsum`

Langkah-langkah pemecahan masalah tambahan melibatkan peninjauan log peristiwa Windows WorkSpaces instance. Peristiwa umum untuk meninjau kegagalan logon adalah Peristiwa 4625: Akun gagal masuk di log Keamanan Windows.

Jika masalah berlanjut, hubungi AWS Support. Untuk informasi lebih lanjut, lihat AWS Support Pusat.

Saya mencoba melakukan sesuatu yang membutuhkan media instalasi Windows tetapi WorkSpaces tidak menyediakannya.

Jika Anda menggunakan bundel publik AWS yang disediakan, Anda dapat menggunakan snapshot EBS media instalasi Windows Server OS yang disediakan oleh Amazon EC2 bila diperlukan.

Buat volume EBS dari snapshot ini, lampirkan ke Amazon EC2, dan transfer file ke tempat file WorkSpace sesuai kebutuhan. Jika Anda menggunakan Windows 10 di BYOL WorkSpaces dan membutuhkan media instalasi, Anda perlu menyiapkan media instalasi Anda sendiri. Untuk informasi selengkapnya, lihat Menambahkan komponen Windows menggunakan media instalasi. Karena Anda tidak dapat langsung melampirkan volume EBS ke a WorkSpace, Anda harus melampirkannya ke instans Amazon EC2 dan menyalin file.

Saya ingin meluncurkan WorkSpaces dengan Direktori AWS Terkelola yang ada yang dibuat di WorkSpaces Wilayah yang tidak didukung.

Untuk meluncurkan Amazon WorkSpaces menggunakan direktori di Wilayah yang saat ini tidak didukung oleh WorkSpaces, ikuti langkah-langkah di bawah ini.

> **Note**
>
> Jika Anda menerima kesalahan saat menjalankan AWS Command Line Interface perintah, pastikan Anda menggunakan AWS CLI versi terbaru. Untuk informasi selengkapnya, lihat Konfirmasi bahwa Anda menjalankan versi terbaru AWS CLI.

Langkah 1: Buat virtual private cloud (VPC) mengintip dengan VPC lain di akun Anda

1. Buat koneksi peering VPC dengan VPC di Wilayah yang berbeda. Untuk informasi selengkapnya, lihat Membuat dengan VPC di akun yang sama dan Wilayah yang berbeda.
2. Terima koneksi peering VPC. Untuk informasi selengkapnya, lihat Menerima koneksi peering VPC.
3. Setelah mengaktifkan koneksi peering VPC, Anda dapat melihat koneksi peering VPC Anda menggunakan konsol VPC Amazon, the, atau API. AWS CLI

Langkah 2: Perbarui tabel rute untuk mengintip VPC di kedua Wilayah

Perbarui tabel rute Anda untuk mengaktifkan komunikasi dengan VPC rekan melalui IPv4 atau IPv6. Untuk informasi selengkapnya, lihat Memperbarui tabel rute untuk koneksi peering VPC.

Langkah 3: Buat AD Connector dan daftarkan Amazon WorkSpaces

1. Untuk meninjau prasyarat AD Connector, lihat Prasyarat AD Connector.
2. Hubungkan direktori Anda yang ada dengan AD Connector. Untuk informasi selengkapnya, lihat Membuat Konektor AD.
3. Jika status AD Connector berubah menjadi Active, buka konsol AWS Directory Service, lalu pilih hyperlink untuk ID Direktori Anda.
4. Untuk AWS aplikasi dan layanan, pilih Amazon WorkSpaces untuk mengaktifkan akses WorkSpaces di direktori ini.
5. Daftarkan direktori dengan WorkSpaces. Untuk informasi selengkapnya, lihat Mendaftarkan direktori dengan WorkSpaces.

Saya ingin memperbarui Firefox di Amazon Linux 2.

Langkah 1: Verifikasi pembaruan otomatis diaktifkan

Untuk memverifikasi bahwa autoupdate diaktifkan, jalankan perintah `systemctl status *os-update-mgmt.timer | grep enabled` pada Anda. WorkSpace Dalam output, harus ada dua baris dengan kata di `enabled` atasnya.

Langkah 2: Memulai pembaruan

Firefox biasanya memperbarui secara otomatis di Amazon Linux 2 WorkSpaces bersama dengan semua paket perangkat lunak lain dalam sistem selama jendela pemeliharaan. Namun, ini tergantung pada jenis yang WorkSpaces Anda gunakan.

- Untuk AlwaysOn WorkSpaces, jendela pemeliharaan mingguan adalah pada hari Minggu 00h00 hingga 04h00, di zona waktu. WorkSpace
- Untuk AutoStop WorkSpaces. dimulai pada hari Senin ketiga setiap bulan, dan hingga dua minggu, jendela pemeliharaan terbuka setiap hari dari sekitar 00h00 hingga 05h00, di zona waktu Wilayah untuk. AWS WorkSpace

Untuk informasi selengkapnya tentang jendela pemeliharaan, lihat WorkSpace pemeliharaan.

Anda juga dapat memulai siklus pembaruan langsung dengan me-reboot WorkSpace dan menghubungkan kembali setelah 15 menit. Anda juga dapat memulai pembaruan dengan memasukkan`sudo yum update`. Untuk memulai pembaruan hanya untuk Firefox, masukkan`sudo yum install firefox`.

Jika Anda tidak dapat mengonfigurasi akses untuk repositori Amazon Linux 2 dan lebih memilih untuk menginstal Firefox menggunakan binari yang dibuat oleh Mozilla, lihat Instal Firefox dari Mozilla build pada dukungan Mozilla. Sebaiknya hapus pemasangan Firefox versi paket RPM sama sekali untuk memastikan Anda tidak menjalankan versi yang sudah ketinggalan zaman karena kesalahan. Anda dapat menghapus instalannya dengan menjalankan perintah`sudo yum remove firefox`.

Anda juga dapat mengunduh paket RPM yang diperlukan dari repositori Amazon Linux 2 dengan menjalankan perintah `yumdownloader firefox` pada mesin yang berbeda. Kemudian, side-load repositori ke WorkSpaces, di mana Anda dapat menginstalnya dengan perintah standar seperti. YUM `sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`

> **Note**
>
> Nama file yang tepat akan berubah berdasarkan versi paket.

Langkah 3: Verifikasi repositori Firefox digunakan

Amazon Linux Extras secara otomatis menyediakan pembaruan Firefox untuk Amazon Linux 2 WorkSpaces. Amazon Linux 2 yang WorkSpaces dibuat setelah 31 Juli 2023 sudah mengaktifkan

repositori Firefox Extra. Untuk memverifikasi bahwa Anda WorkSpace menggunakan repositori Firefox Extra, jalankan perintah berikut.

```
yum repolist | grep amzn2extra-firefox
```

Output perintah akan terlihat seperti `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10` jika repositori Firefox Extra digunakan. Ini akan kosong jika repositori Firefox Extra tidak digunakan. Jika repositori Firefox Extra tidak digunakan, Anda dapat mencoba mengaktifkannya secara manual dengan perintah berikut:

```
sudo amazon-linux-extras install firefox
```

Jika aktivasi repositori Firefox Extra masih gagal, periksa akses internet Anda dan pastikan titik akhir VPC Anda tidak dikonfigurasi. Untuk terus menerima pembaruan Firefox untuk Amazon Linux 2 WorkSpaces melalui repositori YUM, pastikan Anda WorkSpaces dapat menjangkau repositori Amazon Linux 2. Untuk informasi lebih lanjut tentang mengakses repositori Amazon Linux 2 tanpa akses internet, lihat artikel pusat pengetahuan ini.

Pengguna saya dapat mengatur ulang kata sandi mereka menggunakan WorkSpaces klien, mengabaikan pengaturan Fine Grained Password Policy (FFGP) yang dikonfigurasi. AWS Managed Microsoft AD

Jika WorkSpaces klien pengguna Anda dikaitkan dengan AWS Managed Microsoft AD, mereka harus mengatur ulang kata sandi mereka menggunakan pengaturan kompleksitas default.

Kata sandi kompleksitas default peka huruf besar/kecil dan panjangnya harus antara 8 dan 64 karakter, inklusif. Ini harus berisi setidaknya satu karakter dari masing-masing kategori berikut:

- Karakter huruf kecil (a-z)
- Karakter huruf besar (A-Z)
- Angka (0-9)
- Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Pastikan kata sandi tidak menyertakan karakter unicode yang tidak dapat dicetak, seperti spasi putih, tab reture carriage, jeda baris, dan karakter null.

Jika organisasi Anda mengharuskan Anda menerapkan FFGP WorkSpaces, hubungi administrator Direktori Aktif untuk mengatur ulang kata sandi pengguna langsung dari Direktori Aktif, bukan klien. WorkSpaces

Kebijakan akhir hidup aplikasi WorkSpaces klien Amazon

Kebijakan Amazon WorkSpaces end of life (EOL) berlaku untuk versi mayor tertentu (dan semua versi minor mereka) WorkSpaces yang tidak lagi menerima dukungan dan tidak lagi diuji kompatibilitasnya dengan versi yang lebih baru.

Siklus hidup versi WorkSpaces klien memiliki tiga fase — dukungan umum, bimbingan teknis, dan akhir masa pakai (EOL). Fase dukungan umum dimulai pada tanggal rilis publik awal WorkSpaces klien dan berlangsung selama durasi tetap. Selama fase dukungan umum, tim WorkSpaces dukungan memberikan dukungan penuh untuk masalah konfigurasi. Resolusi cacat dan permintaan fitur diimplementasikan untuk versi utama tersebut dan versi minor WorkSpaces klien yang terkait.

Bimbingan teknis diberikan dari akhir fase dukungan umum hingga tanggal EOL. Selama fase bimbingan teknis, Anda menerima dukungan dan bimbingan untuk konfigurasi yang didukung saja. Resolusi cacat dan permintaan fitur diimplementasikan untuk versi terbaru WorkSpaces klien saja. Mereka tidak diimplementasikan untuk versi yang lebih lama. Selama fase panduan teknis, jika perbaikan diperlukan, AWS akan menjadwalkan perbaikan itu untuk rilis versi yang tersedia untuk umum mendatang, dan Anda akan memiliki opsi untuk meningkatkan ke WorkSpaces versi terbaru untuk menerima dukungan terkait dengan perbaikan.

EOL untuk versi mayor terjadi ketika dukungan umum dan bimbingan teknis telah berakhir. Setelah tanggal EOL, tidak ada dukungan atau pemeliharaan lebih lanjut yang diberikan. AWSberhenti menguji masalah kompatibilitas. Untuk dukungan berkelanjutan, Anda harus meningkatkan ke versi WorkSpaces klien terbaru.

Lihat tabel ini untuk informasi selengkapnya tentang dukungan untuk versi tertentu.

Klien Windows	Dukungan umum	Bimbingan teknis	EOL
2.x	2018	Maret 31, 2023	Agustus 31, 2023

Klien Linux	Dukungan umum	Bimbingan teknis	EOL
4.x untuk Ubuntu 18.04	Agustus 12, 2021	Maret 31, 2023	Agustus 31, 2023

Klien Linux	Dukungan umum	Bimbingan teknis	EOL
3.x untuk Ubuntu 18.04	25 November 2019	Maret 31, 2023	Agustus 31, 2023

Klien macOS	Dukungan umum	Bimbingan teknis	EOL
2.x	2019	Maret 31, 2023	Agustus 31, 2023
1.x	2018	Maret 31, 2023	Agustus 31, 2023

Klien iPad	Dukungan umum	Bimbingan teknis	EOL
1.x	2018	Maret 31, 2023	Agustus 31, 2023

Klien Android	Dukungan umum	Bimbingan teknis	EOL
2.x	2019	Maret 31, 2023	Agustus 31, 2023
1.x	2018	Maret 31, 2023	Agustus 31, 2023

Akses web	Dukungan umum		
Google Chrome	Versi saat ini, ditambah dua versi utama terbaru		
Firefox	Versi saat ini, ditambah dua versi utama terbaru		

Akses web	Dukungan umum		
Microsoft Edge	Versi saat ini, ditambah dua versi utama terbaru		

Klien yang tidak didukung

WorkSpaces Klien berikut tidak didukung.

Sistem operasi	Versi klien	Dukungan umum	Bimbingan teknis	EOL	Catatan
Windows	5.11	Juli 3, 2023	Oktober 1, 2023	Oktober 1, 2023	Tidak didukung karena masalah kualitas
Windows	5.10	Juni 19, 2023	Oktober 1, 2023	Oktober 1, 2023	Tidak didukung karena masalah kualitas
Windows	5.9	9 Mei 2023	Oktober 1, 2023	Oktober 1, 2023	Tidak didukung karena masalah kualitas

EOL FAQ

Saya menggunakan versi WorkSpaces klien yang telah mencapai EOL-nya. Apa yang harus saya lakukan untuk meningkatkan ke versi yang didukung?

Buka halaman unduhan WorkSpaces klien untuk mengunduh dan menginstal versi yang didukung penuh dari WorkSpaces.

Dapatkah saya menggunakan versi WorkSpaces klien yang telah mencapai EOL dengan dukungan? WorkSpace

Kami sangat menyarankan untuk meningkatkan klien Anda ke versi terbaru karena resolusi dan fitur sebelumnya tidak lagi diterapkan pada versi klien yang telah mencapai EOL mereka. Jika Anda menggunakan versi klien yang telah mencapai EOL-nya, hubungi tim AWS dukungan untuk informasi lebih lanjut.

Saya menggunakan versi WorkSpaces klien yang telah mencapai EOL-nya. Masih bisakah saya melaporkan masalah untuk itu?

Anda harus terlebih dahulu memutakhirkan ke versi yang didukung dan mencoba mereproduksi masalah tersebut. Jika masalah berlanjut dalam versi yang didukung, buka kasus dukungan dengan tim AWS dukungan.

Saya menggunakan versi WorkSpaces klien yang didukung pada sistem operasi yang telah mencapai EOL-nya. Masih bisakah saya melaporkan masalah untuk itu?

Bantuan teknis dan pembaruan perangkat lunak tidak lagi tersedia untuk sistem operasi yang telah mencapai EOL dan AWS tidak memberikan dukungan kepada WorkSpaces klien yang menggunakan sistem operasi yang telah mencapai EOL-nya. Gunakan sistem operasi yang didukung untuk memastikan Anda memiliki dukungan untuk WorkSpaces klien Anda.

WorkSpaces Kuota Amazon

Amazon WorkSpaces menyediakan berbagai sumber daya yang dapat Anda gunakan di akun Anda di Wilayah tertentu, termasuk gambar WorkSpaces, bundel, direktori, alias koneksi, dan grup kontrol IP. Saat Anda membuat akun Amazon Web Services, kami menetapkan kuota default (juga disebut sebagai batas) pada jumlah sumber daya yang dapat Anda buat.

Berikut ini adalah kuota default WorkSpaces untuk AWS akun Anda. Anda dapat menggunakan konsol Service Quotas untuk melihat kuota default dan kuota yang diterapkan, atau untuk meminta peningkatan kuota untuk kuota yang dapat disesuaikan.

Di beberapa Wilayah, di mana Service Quotas tidak tersedia, Anda harus mengirimkan kasus dukungan untuk meminta peningkatan batas. Untuk informasi selengkapnya, lihat Melihat kuota layanan dan Meminta peningkatan kuota dalam Panduan Pengguna Service Quotas.

Sumber daya	Default	Deskripsi	Dapat disesuaikan
WorkSpaces	1	Jumlah maksimum WorkSpaces dalam akun ini di Wilayah saat ini.	Ya
Grafis WorkSpaces	0	Jumlah maksimum Grafik WorkSpaces di akun ini di Wilayah saat ini. **Note** Bundel grafis tidak lagi didukung setelah 30 November 2023. Kami merekomendasikan untuk	Ya

Sumber daya	Default	Deskripsi	Dapat disesuaikan
		memigrasikan paket Anda WorkSpaces ke Graphics. g4dn. Untuk informasi selengkapnya, lihat Migrasi a WorkSpace.	
Graphics.g4dn WorkSpaces	0	Jumlah maksimum Graphics.g4dn WorkSpaces di akun ini di Wilayah saat ini.	Ya
GraphicsPro WorkSpaces	0	Jumlah maksimum GraphicsPro WorkSpaces dalam akun ini di Wilayah saat ini.	Ya
GraphicsPro.g4dn WorkSpaces	0	Jumlah GraphicsP ro maksimum.g4dn WorkSpaces di akun ini di Wilayah saat ini.	Ya
Siaga WorkSpaces	0	Jumlah maksimum WorkSpaces dalam akun ini di Wilayah saat ini.	Ya

Sumber daya	Default	Deskripsi	Dapat disesuaikan
Paket	50	Jumlah maksimum paket dalam akun di Wilayah saat ini. Kuota ini hanya berlaku untuk paket khusus, bukan untuk paket publik.	Tidak
Alias hubungan	20	Jumlah maksimum alias hubungan di akun di Wilayah saat ini.	Tidak
Direktori	50	Jumlah maksimum direktori yang dapat didaftarkan untuk digunakan dengan Amazon WorkSpaces di akun ini di Wilayah saat ini.	Tidak
Citra	40	Jumlah maksimum citra di akun di Wilayah saat ini.	Ya
Grup kontrol akses IP	100	Jumlah maksimum grup kontrol akses IP di akun di Wilayah saat ini.	Tidak
Grup kontrol akses IP per direktori	25	Jumlah maksimum grup kontrol akses IP per direktori di akun di Wilayah saat ini.	Tidak

Sumber daya	Default	Deskripsi	Dapat disesuaikan
Aturan per grup kontrol akses IP	10	Jumlah maksimum aturan per grup kontrol akses IP di akun di Wilayah saat ini.	Tidak

Pelambatan API

Tarif yang diizinkan adalah dua panggilan per detik. Untuk informasi selengkapnya, lihat Melambatkan pengecualian.

WorkSpaces Versi agen host Protokol Streaming (WSP)

Agen host WorkSpaces Streaming Protocol (WSP) adalah agen host yang berjalan di dalam Anda WorkSpace. Ini mengalirkan piksel Anda WorkSpace ke aplikasi klien dan mencakup fitur dalam sesi, seperti audio dan video dua arah, dan pencetakan. Untuk informasi selengkapnya tentang Protokol WorkSpaces Streaming (WSP), lihat Protokol untuk Amazon. WorkSpaces

Kami menyarankan agar perangkat lunak agen host Anda diperbarui dengan versi terbaru. Anda dapat me-reboot secara manual WorkSpaces untuk memperbarui agen host WSP. Agen host WSP juga diperbarui secara otomatis selama jendela pemeliharaan WorkSpaces default reguler. Untuk informasi selengkapnya tentang jendela pemeliharaan, lihat WorkSpace pemeliharaan. Beberapa fitur ini memerlukan versi WorkSpaces klien terbaru. Untuk informasi selengkapnya tentang versi klien terbaru, lihat WorkSpaces Klien.

Tabel berikut menjelaskan perubahan dalam setiap versi agen host WSP.

Rilis	Tanggal	Perubahan
• Ubuntu WorkSpaces - 2.1.0.1342	Februari 29, 2024	• Mengubah resolusi webcam pilihan menjadi antara 480x360 dan 640x480. • Perbaikan bug dan peningkatan performa.
• Windows WorkSpaces - 2.0.0.1425	Februari 22, 2024	• Menambahkan dukungan untuk permintaan WebAuthn pengalihan dalam sesi dari aplikasi web yang berjalan di browser Google Chrome atau Microsoft Edge jarak jauh. Fitur ini menambahkan prompt browser satu kali yang meminta pengguna untuk mengaktifkan Ekstensi Pengalihan DCV WebAuthn . Ini hanya didukung pada Windows

Rilis	Tanggal	Perubahan
		WorkSpaces dan klien WorkSpaces asli. • Memperbaiki masalah di mana layar putih atau beku terkadang muncul saat masuk. • Perbaikan bug dan peningkatan performa.
• Windows WorkSpaces - 2.0.0.1304	Januari 11, 2024	• Memperbaiki bug yang terkait dengan potensi pembekuan streaming selama login. • Memperbaiki bug terkait pencatatan.
• Windows WorkSpaces - 2.0.0.1288	16 November 2023	• Menambahkan dukungan untuk Indirect Display Driver (IDD) pada Windows 10+, yang menurunkan konsumsi CPU dan meningkatkan kinerja streaming. • Menambahkan pengaturan Kebijakan Grup baru untuk mengaktifkan atau menonaktifkan driver IDD. • Memperbaiki bug yang terkait dengan transparansi gambar clipboard. • Memperbaiki bug yang melestarikan faktor skala Windows. • Perbaikan bug dan peningkatan performa.

Rilis	Tanggal	Perubahan
• Windows WorkSpaces - 2.0.0.1164	Oktober 13, 2023	• Menambahkan dukungan untuk VSync di driver tampilan virtual. • Menambahkan pengaturan Kebijakan Grup baru untuk mengaktifkan atau menonaktifkan vSync. • Masalah koneksi ulang dan keandalan yang ditingkatkan. • Perbaikan bug dan peningkatan performa.
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu WorkSpaces - 2.1.0.1086	18 Agustus 2023	• Menambahkan pengaturan baru untuk mengaktifkan atau menonaktifkan pengalihan zona waktu. • Memperpanjang batas waktu masuk dan menambahkan opsi konfigurasi. • Gerbang yang ditingkatkan untuk memungkinkan koneksi ulang yang lebih cepat setelah gangguan. • Perbaikan bug dan peningkatan performa.

Rilis	Tanggal	Perubahan
• Amazon Linux WorkSpaces - 2.0.0.907	Juni 30, 2023	• Menambahkan dukungan untuk SDK Ekstensi DCV untuk mengaktifkan integrasi khusus ISV. • Mengubah perilaku pemutusan sehingga logout mengakhiri sesi pengguna. • Menambahkan dukungan untuk pengalihan zona waktu. • Memperpanjang batas waktu masuk dan menambahkan opsi konfigurasi. • Memperbaiki masalah upgrade. • Perbaikan bug dan peningkatan performa.
• Windows WorkSpaces - 2.0.0.829	8 Juni 2023	• Mengubah perilaku pemutusan sehingga logout mengakhiri sesi pengguna. • Memperbaiki bug yang terkait dengan sinkronisasi A/V dan keyboard Jepang. • Peningkatan keandalan installer WSP.
• Ubuntu WorkSpaces - 2.1.0.829	16 Mei 2023	• Mengubah perilaku pemutusan sehingga logout mengakhiri sesi pengguna. • Menambahkan dukungan untuk SDK Ekstensi DCV untuk mengaktifkan integrasi khusus ISV. • Menambahkan dukungan untuk pengalihan zona waktu. • Memperbaiki masalah upgrade.

Rilis	Tanggal	Perubahan
• Windows WorkSpaces - 2.0.0.799	8 Mei 2023	• Transportasi QUIC berbasis UDP yang disempurnakan dengan beberapa kualitas gambar dan pengoptimalan kinerja. • Menambahkan dukungan untuk SDK Ekstensi DCV untuk mengaktifkan integrasi khusus ISV. • Menambahkan pengaturan Kebijakan Grup baru untuk mengaktifkan atau menonaktifkan SDK Ekstensi. • Tata letak keyboard Korea, Jepang, dan Jerman yang ditingkat kan. • Memperbaiki bug yang terkait dengan masalah pembekuan sesi, akselerasi perangkat keras, pengalihan printer, verbositas log, dan pengaturan Kebijakan Grup target-fps.

Note

- Untuk informasi tentang cara memeriksa versi agen host Anda, lihat Sistem operasi klien dan host apa yang didukung oleh WSP versi terbaru? .
- Untuk informasi tentang cara memperbarui versi agen host Anda, lihat Jika saya sudah memiliki WSP WorkSpace, bagaimana cara memperbaruinya? .
- Untuk catatan rilis versi klien macOS WSP, lihat Catatan rilis di bagian aplikasi klien WorkSpaces macOS di Panduan Pengguna. WorkSpaces
- Untuk catatan rilis versi klien WSP Windows, lihat Catatan rilis di bagian aplikasi klien WorkSpaces Windows dari Panduan WorkSpaces Pengguna.

Ekstensi SDK didukung oleh WSP

Amazon WorkSpaces Streaming Protocol (WSP) dibuat menggunakan teknologi NICE DCV, memungkinkan akses jarak jauh berkinerja tinggi WorkSpaces ke instans untuk berbagai beban kerja dan kasus penggunaan. Dengan NICE DCV Extension SDK, pengembang dapat menyesuaikan WorkSpaces pengalaman WSP untuk pengguna akhir, termasuk:

- Memfasilitasi dukungan perangkat keras khusus.
- Meningkatkan kegunaan aplikasi pihak ketiga dalam sesi jarak jauh. Misalnya, menambahkan penghentian audio lokal untuk aplikasi VoIP atau pemutaran video lokal untuk aplikasi konferensi
- Menyediakan perangkat lunak aksesibilitas seperti pembaca layar dengan informasi tentang sesi jarak jauh dan aplikasi yang berjalan dari jarak jauh.
- Memungkinkan perangkat lunak keamanan untuk menganalisis postur keamanan titik akhir lokal untuk memungkinkan kebijakan akses bersyarat.
- Melakukan transfer data sewenang-wenang melalui sesi jarak jauh yang telah ditetapkan.

Untuk memulai dengan SDK Ekstensi DCV NICE, lihat Dokumentasi SDK Ekstensi DCV NICE DCV. Anda dapat menemukan SDK itu sendiri di repositori SDK Ekstensi GitHub NICE DCV. Selain itu, Anda juga dapat menemukan contoh integrasi SDK di repositori sampel SDK Ekstensi DCV NICE DCV. GitHub

Berikut ini didukung oleh WorkSpaces.

- Protokol streaming - Protokol WorkSpaces Streaming (WSP)
- WorkSpaces Klien Windows — Windows: 5.9.0.4110 dan di atas.

> **Note**
>
> WorkSpaces Klien Android, iOS, akses web tidak mendukung SDK Ekstensi DCV NICE.

- WorkSpaces didukung - Windows, Linux, dan server Ubuntu

Riwayat dokumen untuk WorkSpaces

Tabel berikut menjelaskan perubahan penting pada WorkSpaces layanan dan Panduan WorkSpaces Administrasi Amazon mulai 1 Januari 2018, dan seterusnya. Kami juga rutin memperbarui dokumentasi untuk menjawab umpan balik yang Anda kirimkan kepada kami.

Untuk pemberitahuan tentang pembaruan ini, Anda dapat berlangganan umpan WorkSpaces RSS.

Perubahan	Deskripsi	Tanggal
AmazonWorkSpacesAdmin pembaruan kebijakan terkelola	WorkSpaces menambahkan ruang kerja: RestoreWorkspace tindakan ke kebijakan AmazonWorkSpacesAdmin terkelola, memberikan akses admin untuk memulihkan. WorkSpaces	Juli 17, 2023
Ekstensi SDK didukung oleh WSP	Dengan NICE DCV Extension SDK, pengembang dapat menyesuaikan WorkSpaces pengalaman WSP untuk pengguna akhir.	25 Mei 2023
WorkSpaces Versi agen host Protokol Streaming (WSP)	Informasi versi untuk WorkSpaces Streaming Protocol (WSP).	8 Mei 2023
Amazon WorkSpaces diluncurkan di AWS GovCloud (AS-Timur)	Amazon WorkSpaces tersedia di AWS GovCloud (AS-Timur).	3 Mei 2023
Dukungan WorkSpaces webcam Amazon	Amazon WorkSpaces sekarang mendukung audio-video real-time (AV) dengan mengarahkan input video webcam lokal secara mulus ke WorkSpaces desktop	5 April 2021

	Windows menggunakan Streaming Protocol (WSP). WorkSpaces	
Dukungan kartu WorkSpaces pintar Amazon dengan aplikasi WorkSpaces klien macOS	Anda sekarang dapat menggunakan aplikasi klien WorkSpaces macOS Amazon dengan kartu pintar Common Access Card (CAC) dan Personal Identity Verification (PIV). Dukungan kartu pintar tersedia saat WorkSpace s menggunakan Protokol WorkSpaces Streaming (WSP).	5 April 2021
API manajemen WorkSpaces bundel Amazon	API manajemen WorkSpace s bundel Amazon sekarang tersedia. Tindakan API ini mendukung pembuatan, penghapusan, dan operasi asosiasi gambar untuk WorkSpaces bundel.	15 Maret 2021
Amazon WorkSpaces diluncurkan di Asia Pasifik (Mumbai)	Amazon WorkSpaces tersedia di Wilayah Asia Pasifik (Mumbai).	8 Maret 2021

WorkSpaces Protokol Streaming (WSP)	Protokol WorkSpaces Streaming (WSP) sekarang tersedia untuk kedua lisensi yang disertakan (Windows Server 2016) dan BYOL Windows 10 WorkSpaces berdasarkan semua jenis bundel kecuali untuk Grafik dan. GraphicsPro WSP juga tersedia untuk Linux WorkSpaces di Wilayah AWS GovCloud (AS-Barat).	1 Desember 2020
Kartu Pintar	Amazon WorkSpaces sekarang mendukung pra-sesi (login) dan otentikas i kartu pintar dalam sesi pada Windows dan Linux WorkSpaces di Wilayah AWS GovCloud (AS-Barat).	1 Desember 2020
Bagikan Gambar Kustom	Anda sekarang dapat berbagi WorkSpaces gambar kustom di seluruh AWS akun. Setelah gambar dibagikan, akun penerima dapat menyalin gambar dan menggunak annya untuk membuat bundel untuk meluncurkan yang baru WorkSpaces.	1 Oktober 2020

Pengalihan Lintas Wilayah	Sekarang Anda dapat menggunakan pengaliha n lintas wilayah, fitur yang berfungsi dengan kebijakan perutean Sistem Nama Domain (DNS) Anda untuk mengarahkan pengguna Anda ke alternatif WorkSpaces saat primer mereka tidak tersedia. WorkSpaces	10 September 2020
Berlangganan Microsoft Office 2016 atau 2019 untuk BYOL WorkSpaces	Anda sekarang dapat berlangganan Microsoft Office Professional 2016 atau 2019 yang disediakan oleh AWS Bring Your Own Windows License (BYOL) WorkSpaces.	3 September 2020
Otomasi BYOL di Tiongkok (Ningxia)	Anda dapat menggunak an otomatisasi Bring Your Own License (BYOL) untuk menyederhanakan proses penggunaan lisensi desktop Windows 10 Anda untuk Anda WorkSpaces di China (Ningxia).	2 April 2020

Pemeriksa Gambar	Alat Pemeriksa Gambar membantu Anda menentukan apakah Windows Anda WorkSpace memenuhi persyaratan untuk pembuatan gambar. Pemeriksa Gambar melakukan serangkaian pengujian WorkSpace yang ingin Anda gunakan untuk membuat gambar Anda, dan memberikan panduan tentang cara mengatasi masalah apa pun yang ditemukannya.	30 Maret 2020
Migrasi WorkSpaces	Fitur WorkSpaces migrasi Amazon memungkinkan Anda untuk memigrasikan WorkSpace dari satu bundel ke bundel lainnya, sambil mempertahankan data pada volume pengguna. Anda dapat menggunakan fitur ini untuk bermigrasi WorkSpaces dari pengalaman desktop Windows 7 ke pengalaman desktop Windows 10. Anda juga dapat menggunakan fitur ini untuk bermigrasi WorkSpaces dari satu bundel publik atau kustom ke bundel lainnya.	9 Januari 2020

PrivateLink integrasi untuk Amazon WorkSpaces API	Anda dapat terhubung langsung ke titik akhir Amazon WorkSpaces API melalui titik akhir antarmuka di Virtual Private Cloud (VPC) alih-alih terhubung melalui internet. Saat Anda menggunakan titik akhir antarmuka VPC, komunikasi antara VPC dan titik akhir Amazon WorkSpace s API dilakukan sepenuhnya dan aman di dalam jaringan. AWS	25 November 2019
Klien Linux untuk Amazon WorkSpaces	Pengguna sekarang dapat menggunakan klien Linux untuk mengakses mereka WorkSpaces.	25 November 2019
Amazon WorkSpaces diluncurkan di China (Ningxia)	Amazon WorkSpaces tersedia di Wilayah China (Ningxia).	13 November 2019
Kembalikan WorkSpaces ke keadaan sehat terakhir yang diketahui	Anda dapat menggunakan fitur pemulihan untuk mengembal ikan WorkSpace ke keadaan sehat terakhir yang diketahui.	18 September 2019

Enkripsi titik akhir FIPS	Untuk mematuhi Federal Risk and Authorization Management Program (FedRAMP) atau Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), Anda dapat mengonfigurasi WorkSpaces Amazon untuk menggunakan enkripsi endpoint Standar Pemrosesan Informasi Federal (FIPS) di tingkat direktori.	12 September 2019
Salin WorkSpace gambar	Anda dapat menyalin citra Anda dalam Wilayah yang sama atau di seluruh Wilayah.	27 Juni 2019
Kemampuan WorkSpace Manajemen Layanan Mandiri untuk Pengguna	Anda dapat mengaktifkan kemampuan WorkSpace manajemen swalayan bagi pengguna Anda untuk memberi mereka kontrol lebih besar atas pengalaman mereka.	19 November 2018
Otomatisasi BYOL	Anda dapat menggunakan otomatisasi Bring Your Own License (BYOL) untuk menyederhanakan proses menggunakan lisensi desktop Windows 7 dan Windows 10 untuk Anda. WorkSpaces	16 Novbucket 2018
PowerPro dan GraphicsPro bundel	GraphicsPro Paket PowerPro dan sekarang tersedia untuk WorkSpaces.	18 Oktober 2018

Pantau WorkSpace login yang berhasil	Anda dapat menggunakan peristiwa dari Amazon CloudWatch Events untuk memantau dan merespons WorkSpace login yang berhasil.	17 September 2018
Akses Web untuk Windows 10 WorkSpaces	Pengguna sekarang dapat menggunakan klien akses web untuk mengakses pengalaman desktop Windows 10 yang WorkSpace berjalan.	24 Agustus 2018
Login URI	Anda dapat menggunakan Uniform Resource Identifiers (URI) untuk menyediakan pengguna dengan akses ke mereka. WorkSpaces	31 Juli 2018
Amazon Linux WorkSpaces	Anda dapat menyediakan Amazon Linux WorkSpaces untuk pengguna Anda.	26 Juni 2018
Grup kontrol akses IP	Anda dapat mengontrol alamat IP dari mana pengguna dapat mengakses mereka WorkSpaces.	30 April 2018
Upgrade di tempat	Anda dapat memutakhirkan Windows 10 BYOL Anda WorkSpaces ke versi Windows 10 yang lebih baru.	9 Maret 2018

Pembaruan Sebelumnya

Tabel berikut menjelaskan penambahan penting pada WorkSpaces layanan Amazon dan dokumentasinya ditetapkan sebelum 1 Januari 2018.

Perubahan	Deskripsi	Tanggal
Opsi komputasi yang fleksibel	Anda dapat beralih di WorkSpaces antara bundel Nilai, Standar, Kinerja, dan Daya	22 Desember 2017
Penyimpanan yang dapat dikonfigurasi	Anda dapat mengonfigurasi ukuran root dan volume pengguna untuk Anda WorkSpaces saat Anda meluncurkannya dan meningkatkan ukuran volume ini nanti.	22 Desember 2017
Kontrol akses perangkat	Anda dapat menentukan jenis perangkat yang memiliki akses ke WorkSpaces. Selain itu, Anda dapat membatasi akses WorkSpaces ke perangkat tepercaya (juga dikenal sebagai perangkat terkelola).	19 Juni 2017
Perwalian antar hutan	Anda dapat membuat hubungan kepercaya an antara iklan Microsoft AWS Terkelola dan domain Microsoft Active Directory lokal, lalu menyediakan WorkSpaces untuk pengguna di domain lokal.	9 Februari 2017
Bundel Windows Server 2016	WorkSpaces menawarkan bundel yang menyertakan pengalaman desktop Windows 10, didukung oleh Windows Server 2016.	29 November 2016
Akses Web	Anda dapat mengakses Windows Anda WorkSpaces dari browser web menggunakan Akses WorkSpaces Web.	18 November 2016
Setiap jam WorkSpaces	Anda dapat mengonfigurasi WorkSpaces sehingga pengguna ditagih per jam.	18 Agustus 2016
Windows 10 BYOL	Anda dapat membawa Lisensi Desktop Windows 10 Anda ke WorkSpaces (BYOL).	21 Juli 2016
Dukungan penandaan	Anda dapat menggunakan tag untuk mengelola dan melacak Anda WorkSpaces.	17 Mei 2016

Perubahan	Deskripsi	Tanggal
Registrasi tersimpan	Setiap kali Anda memasukkan kode pendaftaran baru, WorkSpaces klien menyimpannya. Ini membuatnya lebih mudah untuk beralih WorkSpaces di direktori atau Wilayah yang berbeda.	28 Januari 2016
Windows 7 BYOL, klien Chromebook, enkripsi WorkSpace	Anda dapat membawa Lisensi Desktop Windows 7 ke WorkSpaces (BYOL), menggunakan klien Chromebook, dan menggunakan enkripsi. WorkSpace	1 Oktober 2015
CloudWatch pemantauan	Menambahkan informasi tentang CloudWatch pemantauan.	28 April 2015
Sesi otomatis menyambung kembali	Menambahkan informasi tentang fitur auto session reconnect di aplikasi klien WorkSpaces desktop.	31 Maret 2015
Alamat IP publik	Anda dapat secara otomatis menetapkan alamat IP publik ke alamat Anda WorkSpaces.	23 Januari 2015
WorkSpaces diluncurkan di Asia Pasifik (Singapura)	WorkSpaces tersedia di Wilayah Asia Pasifik (Singapura).	15 Januari 2015
Nilai bundel ditambahkan, pembaruan bundel Standar, Office 2013 ditambahkan	Paket Nilai tersedia, perangkat keras paket Standar telah ditingkatkan, dan Microsoft Office 2013 tersedia dalam paket Plus.	6 November 2014
Dukungan gambar dan bundel	Anda dapat membuat gambar dari WorkSpace yang telah Anda sesuaikan dan WorkSpace bundel khusus dari gambar.	28 Oktober 2014
PCoIP nol dukungan klien	Anda dapat mengakses perangkat klien nol WorkSpaces PCoIP.	15 Oktober 2014
WorkSpaces Diluncurkan di Asia Pasifik (Tokyo)	WorkSpaces tersedia di Wilayah Asia Pasifik (Tokyo).	26 Agustus 2014

Perubahan	Deskripsi	Tanggal
Dukungan printer lokal	Anda dapat mengaktifkan dukungan printer lokal untuk Anda WorkSpaces.	26 Agustus 2014
Otentikasi multi-faktor	Anda dapat menggunakan autentikasi multi-faktor dalam direktori yang terhubung.	11 Agustus 2014
Dukungan OU default dan dukungan domain target	Anda dapat memilih Unit Organisasi (OU) default tempat akun WorkSpace mesin Anda ditempatkan, dan domain terpisah tempat akun WorkSpace mesin Anda dibuat.	7 Juli 2014
Tambahkan grup keamanan	Anda dapat menambahkan grup keamanan ke grup Anda WorkSpaces.	7 Juli 2014
WorkSpaces Diluncurkan di Asia Pasifik (Sydney)	WorkSpaces tersedia di Wilayah Asia Pasifik (Sydney).	15 Mei 2014
WorkSpaces diluncurkan di Eropa (Irlandia)	WorkSpaces tersedia di Wilayah Eropa (Irlandia).	5 Mei 2014
Beta publik	WorkSpaces tersedia sebagai beta publik.	25 Maret 2014

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