

Panduan Administrator

# Amazon Nimble Studio



# Amazon Nimble Studio: Panduan Administrator

Copyright © 2020 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

---

# Table of Contents

Apa itu Nimble Studio? .....	1
Fitur dan manfaat .....	1
Aplikasi terkait .....	2
Harga untuk Nimble Studio .....	2
Memulai dengan Nimble Studio .....	3
Konsep dan terminologi .....	4
Fitur kunci .....	4
Konsep dan terminologi utama .....	5
Pengaturan .....	8
Menyiapkan IAM .....	8
Mendaftar untuk Akun AWS .....	8
Buat pengguna dengan akses administratif .....	9
Sumber daya terkait .....	10
Mulai .....	11
Pengaturan cepat .....	11
Langkah 1: Konfigurasi infrastruktur studio .....	11
Langkah 2: Tinjau dan buat studio Anda .....	12
Pengaturan tambahan .....	12
Konfigurasi peran pengguna studio .....	13
AWS IAM Identity Center .....	14
Konfigurasi kunci AWS KMS enkripsi .....	14
Konfigurasi Tanda .....	15
Menghapus hapus hapus hapus hapus hapus Studio .....	16
Keamanan .....	17
Informasi Selengkapnya .....	17
Keamanan akun .....	18
Hapus kunci akses akun Anda .....	18
Mengaktifkan autentikasi multi-faktor .....	18
Aktifkan CloudTrail di semua Wilayah AWS .....	19
Siapkan Amazon GuardDuty dan notifikasi .....	19
Perlindungan data .....	22
Enkripsi diam .....	23
Enkripsi bergerak .....	24
Manajemen kunci untuk Amazon Nimble Studio .....	24

Langkah-langkah keamanan data .....	25
Data diagnostik dan metrik .....	26
Identity and Access Management .....	27
Audiens .....	27
Mengautentikasi dengan identitas .....	28
Mengelola akses menggunakan kebijakan .....	30
Bagaimana Amazon Nimble Studio bekerja dengan IAM .....	33
Contoh kebijakan berbasis ID .....	39
AWS kebijakan terkelola .....	41
Pencegahan confused deputy lintas layanan .....	50
Pemecahan Masalah .....	52
Pencatatan dan pemantauan .....	55
Logging panggilan Nimble Studio menggunakan AWS CloudTrail .....	55
Validasi kepatuhan .....	61
Keamanan infrastruktur .....	63
Praktik terbaik keamanan .....	63
Pemantauan .....	63
Perlindungan data .....	64
Izin .....	64
Dukungan .....	65
Nimble ble ble ble ble ble ble ble ble ble .....	65
Dukungan aplikasi .....	65
AWSThinkboxDeadline .....	65
Nimble ble ble ble ble ble ble ble File Transfer .....	65
AWS SupportPusat .....	65
AWS Supportrencana .....	66
Riwayat dokumen .....	67
AWSGlosarium .....	68
.....	Ixix

# Apa itu Amazon Nimble Studio?

Nimble Studio menyediakan infrastruktur dan manajemen terpusat untuk serangkaian aplikasi dan layanan yang dapat digunakan seniman untuk menghasilkan efek visual, animasi, dan konten game di cloud.

Dengan Nimble Studio, Anda mendapatkan alat penting untuk manajemen pengguna dan grup. Anda juga dapat menambah dan mengelola aplikasi, termasuk AWS Thinkbox dan Nimble Studio File Transfer.

Nimble Studio memiliki antarmuka terpadu yang menempatkan semua sumber daya studio Anda di satu tempat. Anda dapat onboard pengguna, menetapkan aplikasi, dan melampirkan izin khusus untuk fungsi pekerjaan mereka. Nimble Studio tidak memerlukan AWS pengalaman, dan Anda dapat mengaturnya dalam waktu sekitar lima menit.

## Daftar Isi

- [Fitur dan manfaat](#)
- [Aplikasi terkait](#)
- [Harga untuk Nimble Studio](#)
- [Memulai dengan Nimble Studio](#)

## Fitur dan manfaat

Berikut adalah beberapa fitur dan manfaat yang Anda dapatkan dengan Nimble Studio:

- Gunakan Nimble Studio tanpa biaya; bayar hanya untuk sumber daya studio yang digunakan aplikasi Anda.
- Kelola studio Anda secara terpusat, periksa statusnya, dan dapatkan wawasan tingkat tinggi tentang operasinya.
- Menambahkan dan mengelola aplikasi Nimble Studio, pengguna dan kelompok, dan melampirkan izin.
- Kelola akses ke sumber daya studio dengan aman dengan kebijakan dan peran AWS Identity and Access Management (IAM).
- Kelola keamanan masuk untuk pengguna studio dan penyedia identitas eksternal dengan AWS IAM Identity Center (IAM Identity Center).

- Atur dan temukan sumber daya studio dengan mudah dengan tag ke sumber daya studio Anda.

## Aplikasi terkait

Nimble Studio menyediakan aplikasi untuk pembuat konten digital untuk mengoperasikan studio berbasis cloud untuk menghasilkan efek visual (VFX), animasi, dan konten interaktif.

Anda dapat menginstal aplikasi ini ke komputer lokal atau di cloud dengan instans Amazon Elastic Compute Cloud (Amazon EC2). Anda juga dapat menggunakan Amazon Simple Storage Service (Amazon S3) untuk mentransfer dan menyimpan aset media digital dengan aman. Ini berarti Anda dapat menggunakan Nimble Studio untuk mengurangi biaya infrastruktur fisik, peralatan, dan staf teknis.

Nimble Studio saat ini menyediakan aplikasi berikut:

- AWSThinkbox: Thinkbox perangkat lunak termasuk Thinkbox Batas waktu manajer pertanian render, dan plugin 3D, Thinkbox Krakatau. Anda dapat menggunakan Thinkbox perangkat lunak untuk membantu Anda meningkatkan output kreatif studio Anda di lokasi, di cloud dengan Amazon EC2, atau kombinasi keduanya. Untuk informasi lebih lanjut, lihat [AWS ThinkboxProduk](#).
- Nimble Studio File Transfer: File Transfer mempercepat transfer aset media aset media digital ke dan dari Amazon S3. File Transfer menyediakan antarmuka pengguna grafis, yang dapat Anda gunakan untuk memindahkan ribuan file media besar dengan cepat. Untuk informasi selengkapnya, lihat Nimble Studio File Transfer halaman [Apa itu](#).

## Harga untuk Nimble Studio

Tidak ada biaya untuk mengatur Nimble Studio dan menggunakannya untuk mengelola infrastruktur studio, pengguna, keamanan, dan layanan Anda.

Namun, jika Anda menyiapkan layanan dan aplikasi di studio Anda, Anda mungkin dikenakan biaya untuk penyimpanan dan sumber daya studio lainnya. Untuk informasi selengkapnya tentang harga aplikasi Nimble Studio, lihat halaman harga aplikasi individual.

Untuk informasi tentang mengelola AWS biaya Anda, lihat [AWS Cost Explorer Service](#) dan [AWS Budgets](#).

# Memulai dengan Nimble Studio

Penyiapan dan penyebaran Studio gesit membutuhkan waktu sekitar lima menit.

Setelah Anda membiasakan diri dengan Nimble Studio [Concepts dan terminologi](#), lihat [Memulai](#) dengan Amazon Nimble Studio. Di dalamnya, Anda akan menemukan step-by-step petunjuk untuk menerapkan studio Anda.

# Konsep dan terminologi untuk Amazon Nimble Studio

Untuk membantu Anda memulai Amazon Nimble Studio, dan memahami cara kerjanya, Anda dapat merujuk ke konsep dan terminologi utama dalam panduan ini.

## Fitur kunci

### Studio Gesit Amazon

Amazon Nimble Studio adalah Layanan AWS studio kreatif untuk menghasilkan efek visual, animasi, dan konten interaktif sepenuhnya di cloud, mulai dari sketsa storyboard hingga hasil akhir.

### Konsol Amazon Nimble Studio

Konsol Studio gesit adalah bagian dari AWS Management Console yang dikhususkan untuk pelanggan TI admin kami. Konsol ini adalah tempat admin membuat studio cloud mereka dan mengelola banyak pengaturan. Misalnya, halaman manajer Studio memungkinkan Anda untuk menambah atau menghapus sumber daya, menambahkan aplikasi, dan memberikan izin kepada pengguna dan grup.

### Portal Studio Gesit Amazon

Portal Nimble Studio menyediakan antarmuka pengguna untuk day-to-day interaksi dengan aplikasi dan layanan Nimble Studio. Pengguna masuk langsung ke portal dengan nama pengguna dan kata sandi mereka tanpa harus berinteraksi dengan AWS Management Console.

### Nimble Studio File Transfer

File Transfer mempercepat transfer aset media digital ke dan dari Amazon Simple Storage Service (Amazon S3). File Transfer menyediakan antarmuka pengguna grafis, yang dapat Anda gunakan untuk memindahkan ribuan file media besar dengan cepat. Untuk informasi selengkapnya, lihat Nimble Studio File Transfer halaman [Apa itu](#).

### AWS Thinkbox

Thinkbox perangkat lunak termasuk membuat manajer pertanian Thinkbox Batas waktu, dan plugin 3D, Thinkbox Krakatau. Anda dapat menggunakan Thinkbox perangkat lunak untuk membantu Anda meningkatkan output kreatif studio Anda di lokasi, di cloud dengan Amazon EC2, atau kombinasi keduanya. Untuk informasi lebih lanjut, lihat [AWS Thinkbox Produk](#).



# Konsep dan terminologi utama

## AWSkebijakan terkelola

Kebijakan yang AWS dikelola adalah kebijakan mandiri yang dibuat dan dikelola olehAWS. Kebijakan mandiri berarti bahwa kebijakan tersebut memiliki Amazon Resource Name (ARN) sendiri yang mencakup nama kebijakan. Misalnya, `arn:aws:iam: :aws:policy/IAM` adalah kebijakan terkelola. `ReadOnlyAccess` AWS Untuk informasi selengkapnya tentang ARN, lihat [ARN IAM](#).

AWSkebijakan terkelola digunakan untuk memberikan izin ke fungsi pekerjaan umum. Kebijakan fungsi pekerjaan dikelola dan diperbarui AWS ketika layanan baru dan operasi API diperkenalkan. Misalnya, fungsi `AdministratorAccess`pekerjaan menyediakan akses penuh dan delegasi izin untuk setiap layanan dan sumber daya di. AWS Sedangkan, kebijakan AWS terkelola akses parsial-seperti `AmazonMobileAnalyticsWriteOnlyAccess` dan `AmazonEC2ReadOnlyAccess` dapat memberikan tingkat akses tertentu tanpa mengizinkan akses penuh. Layanan AWS Untuk mempelajari lebih lanjut tentang kebijakan akses, lihat [Memahami ringkasan tingkat akses dalam ringkasan kebijakan](#).

## AWS Management Console

[AWS Management Console](#)Ini adalah aplikasi web yang menyediakan akses ke koleksi luas konsol layanan untuk mengelolaLayanan AWS.

Setiap layanan juga mencakup konsolnya sendiri. Konsol ini menawarkan berbagai alat untuk komputasi awan. Bahkan ada layanan yang membantu dengan [penagihan dan manajemen biaya](#).

## AWS IAM Identity Center(Pusat Identitas IAM)

IAM Identity Center adalah AWS layanan yang memudahkan pengelolaan akses terpusat ke beberapa Akun AWS aplikasi bisnis. Dengan IAM Identity Center, Anda dapat memberi pengguna akses masuk tunggal ke semua akun dan aplikasi yang ditetapkan dari satu tempat. Anda juga dapat mengelola akses multi-akun dan izin pengguna secara terpusat ke semua akun Anda. AWS Organizations Untuk informasi lebih lanjut, kunjungi [AWS IAM Identity CenterFAQ](#).

## AWS PrivateLink

AWSPrivateLinkmenyediakan konektivitas pribadi antara VPC,Layanan AWS, dan jaringan lokal Anda, tanpa mengekspos lalu lintas Anda ke internet publik. AWS PrivateLinkmemudahkan untuk menghubungkan layanan di berbagai akun dan VPC. [AWS PrivateLink](#)tersedia untuk biaya bulanan yang ditagihkan kepada AndaAkun AWS.

## Pembuatan Konten Digital (DCC)

Digital Content Creation (DCC) mengacu pada kategori aplikasi yang digunakan untuk menghasilkan konten kreatif, termasuk, Blender, NukeMaya, dan Houdini.

## Daerah

Lincah Studio menawarkan sebelas Wilayah AWS dari yang untuk memilih menyebarkan studio Anda. Wilayah adalah tempat infrastruktur studio penting ada, seperti data dan aplikasi Anda.

Wilayah harus terletak paling dekat dengan pengguna studio Anda. Ini mengurangi lag dan meningkatkan kecepatan transfer data.

## Studio

Studio adalah wadah tingkat atas untuk sumber daya terkait Nimble Studio lainnya. Studio cloud Anda mengelola portal web Nimble Studio dan koneksi ke sumber daya penting di Akun AWS seperti kunci enkripsi VPC, direktori pengguna, dan penyimpanan Anda.

## Aplikasi studio

Komponen Studio adalah konfigurasi dalam Nimble Studio pelanggan yang memberitahu layanan bagaimana mengakses sumber daya seperti sistem file, server lisensi, dan membuat peternakan di Akun AWS

Nimble Studio berisi sejumlah sub tipe komponen studio termasuk sistem file bersama, pertanian komputasi, Active Directory, dan komponen lisensi. Sub tipe ini menjelaskan sumber daya yang Anda ingin studio Anda gunakan.

## Sumber daya studio

Sumber daya studio adalah istilah yang merangkum hal-hal yang dibutuhkan studio dalam operasi sehari-hari mereka. Ketika menjelaskan bagaimana sumber daya cocok dengan infrastruktur studio cloud, mereka mungkin juga disebut sebagai komponen studio.

## Tag

Tanda merupakan sebuah label yang Anda tetapkan ke sebuah sumber daya AWS. Setiap tag terdiri dari kunci dan nilai opsional yang Anda tentukan.

Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda. Misalnya, Anda dapat menentukan serangkaian tag untuk instans Amazon Elastic Compute Cloud (Amazon EC2) akun Anda yang membantu Anda melacak setiap pemilik instans dan tingkat

tumpukan. Tag juga memungkinkan Anda untuk mengintegrasikan sistem file bersama organisasi Anda dan membuat peternakan dengan Nimble Studio, untuk menjaga alur kerja Anda tidak terganggu saat Anda memindahkan tenaga kerja Anda ke cloud.

Dengan tag, Anda dapat mengkategorikan AWS sumber daya Anda berdasarkan tujuan, pemilik, atau lingkungan. Ini berguna ketika Anda memiliki banyak sumber daya dengan jenis yang sama—Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang telah Anda tetapkan padanya.

# Menyiapkan untuk Nimble Studio

Tutorial ini untuk pengguna administrator yang ingin menyiapkan Amazon Nimble Studio.

Bagian berikut akan memandu Anda melalui langkah-langkah yang perlu Anda selesaikan sebelum menyebarkan studio di Nimble Studio.

Daftar Isi

- [Menyiapkan IAM](#)
- [Sumber daya terkait](#)

## Menyiapkan IAM

Tinjau dokumentasi AWS Identity and Access Management (IAM) berikut sebelum Anda mulai.

- [Praktik terbaik keamanan di IAM](#)
- Masuk ke Akun AWS sebagai pengguna admin untuk menyelesaikan persiapan yang tersisa.

## Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

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

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

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

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

## Buat pengguna dengan akses administratif

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

### Amankan Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

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

### Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

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

### Masuk sebagai pengguna dengan akses administratif

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

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

Tetapkan akses ke pengguna tambahan

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

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

## Sumber daya terkait

- [Praktik Terbaik Keamanan di IAM](#)
- [Layanan AWS kuota - Referensi Umum AWS](#)

# Memulai dengan Amazon Nimble Studio

Bab ini menunjukkan cara menggunakan konsol Nimble Studio untuk membuat infrastruktur studio Anda, mengonfirmasi, meninjau pengaturan Wilayah AWS, dan membuat studio Anda. Anda juga dapat menyesuaikan pengaturan dengan pengaturan tambahan.

Untuk AWS pelanggan pertama kali, lihat [Menyiapkan untuk Nimble Studio](#) tutorialnya.

Topik

- [Menyiapkan Nimble Studio](#)
- [Pengaturan studio tambahan](#)

## Menyiapkan Nimble Studio

Panduan ini menunjukkan cara mengonfigurasi infrastruktur, meninjau pengaturan, dan membuat studio. Anda juga dapat menyesuaikan studio dengan [Pengaturan studio tambahan](#).

### Langkah 1: Konfigurasikan infrastruktur studio

Infrastruktur studio terdiri dari komponen-komponen berikut:

- Nama tampilan studio: Nama tampilan Studio adalah bagaimana Anda dapat mengidentifikasi studio Anda - misalnya AnyCompanyStudio. Nama studio Anda juga menentukan URL portal Studio Anda. Anda dapat mengubah nama tampilan Studio setelah Anda menyelesaikan persiapan, kapan saja.
- URL portal studio: Anda dapat mengakses studio Anda dengan menggunakan URL portal Studio. URL didasarkan pada nama tampilan Studio - misalnya <https://anycompanystudio.awsapps.com>. Anda dapat mengubah URL portal Studio setelah Anda menyelesaikan persiapan, kapan saja.
- Wilayah AWS: Wilayah AWS itu adalah lokasi fisik untuk kumpulan pusat AWS data. Ketika Anda mengatur studio Anda, Region default ke lokasi terdekat dengan Anda. Anda harus mengubah Wilayah sehingga terletak paling dekat dengan pengguna Anda. Ini mengurangi jeda dan meningkatkan kecepatan transfer data.

#### Important

Anda tidak dapat mengubah Wilayah setelah Anda selesai mengonfigurasi Nimble Studio.

Selesaikan tugas di bagian ini untuk mengonfigurasi infrastruktur studio Anda.

Untuk mengonfigurasi infrastruktur studio Anda

1. Masuk ke AWS Management Console dan buka konsol [Nimble Studio](#).
2. Pilih Setup Nimble Studio, lalu pilih Berikutnya.
3. Masukkan nama tampilan Studio — misalnya **AnyCompany Studio**.
4. (Opsional) Untuk mengubah nama portal Studio, pilih Edit URL.
5. (Opsional) Untuk mengubah Wilayah AWS sehingga paling dekat dengan pengguna studio Anda, pilih Ubah Wilayah.
  - a. Pilih Wilayah yang paling dekat dengan pengguna Anda.
  - b. Pilih Terapkan Wilayah.
6. (Opsional) Untuk lebih menyesuaikan pengaturan studio Anda, pilih [Pengaturan studio tambahan](#).
7. Untuk meninjau pengaturan sebelum membuat studio, pilih Berikutnya.

## Langkah 2: Tinjau dan buat studio Anda

Setelah mengonfigurasi infrastruktur studio, Anda dapat meninjau, membuat perubahan, dan membuat studio.

Untuk meninjau dan membuat studio Anda

1. Pada halaman Tinjau dan buat, tinjau infrastruktur Studio Anda.
2. Konfirmasikan bahwa Wilayah AWS yang paling dekat dengan pengguna studio Anda.
3. (Opsional) Pilih Edit untuk membuat perubahan pada penyiapan studio Anda.
4. Saat Anda siap, pilih Buat studio.

## Pengaturan studio tambahan

Penyiapan Studio gesit mencakup pengaturan studio tambahan. Dengan pengaturan ini, Anda dapat melihat semua perubahan Nimble Studio setup membuat Anda Akun AWS, mengkonfigurasi peran pengguna studio Anda, dan mengubah jenis kunci enkripsi Anda. Anda juga dapat menambahkan tanda opsional ke sumber daya.



## Konfigurasi peran pengguna studio

AWS Layanan dapat mengambil peran layanan untuk kemudian melakukan tindakan atas nama Anda. Nimble Studio membutuhkan peran pengguna studio untuk itu untuk memberikan pengguna akses ke sumber daya di studio Anda.

Anda dapat melampirkan kebijakan yang dikelola AWS Identity and Access Management (IAM) ke peran pengguna studio. Kebijakan ini memungkinkan pengguna untuk melakukan tindakan tertentu, seperti membuat pekerjaan dalam aplikasi Nimble Studio tertentu. Karena aplikasi bergantung pada kondisi tertentu dalam kebijakan terkelola, jika Anda tidak menggunakan kebijakan terkelola, aplikasi mungkin tidak berfungsi seperti yang diharapkan.

Anda dapat mengubah peran pengguna studio setelah Anda menyelesaikan pengaturan, kapan saja. Untuk informasi selengkapnya tentang peran pengguna, lihat [Peran IAM](#).

Tab berikut berisi petunjuk untuk dua kasus penggunaan yang berbeda. Untuk membuat dan menggunakan peran layanan baru, pilih tab Peran layanan baru. Untuk menggunakan peran layanan yang ada, pilih tab Peran layanan yang ada.

### New service role

Membuat dan menggunakan peran layanan baru

1. Pilih Buat dan gunakan peran layanan baru.
2. (Opsional) Masukkan nama peran pengguna Layanan.
3. Pilih Lihat detail izin untuk informasi selengkapnya tentang peran tersebut.

### Existing service role

Menggunakan peran layanan yang ada

1. Pilih Gunakan peran layanan yang ada.
2. Buka daftar dropdown untuk memilih peran layanan yang ada.
3. (Opsional) Pilih Tampilan di konsol IAM untuk informasi selengkapnya tentang peran tersebut.

## AWS IAM Identity Center

AWS IAM Identity Center adalah layanan sistem masuk tunggal berbasis cloud untuk mengelola pengguna dan grup. IAM Identity Center juga dapat diintegrasikan dengan penyedia single sign-on (SSO) perusahaan Anda sehingga pengguna dapat masuk dengan akun perusahaan mereka.

Nimble Studio memungkinkan IAM Identity Center secara default, dan diperlukan untuk mengatur dan menggunakan Nimble Studio. Untuk informasi lebih lanjut, lihat [Apa yang dimaksud dengan AWS IAM Identity Center](#).

## Konfigurasi kunci AWS KMS enkripsi

AWS Key Management Service (AWS KMS) kunci adalah jenis kunci KMS yang dapat digunakan untuk mengenkripsi, mendekripsi, dan mengenkripsi ulang data Anda.

Nimble Studio mencakup jenis kunci AWS KMS enkripsi berikut:

- **AWS kunci yang dimiliki AWS** - kunci yang dimiliki adalah kunci KMS yang Layanan AWS dimiliki dan dikelola untuk digunakan dalam beberapa akun AWS. Kunci yang dimiliki tidak ada di akun Anda, tetapi Nimble Studio dapat menggunakan kunci yang dimiliki AWS untuk melindungi sumber daya di akun Anda.

Untuk menggunakannya AWS KMS, Anda tidak perlu membuat atau mempertahankan kunci atau kebijakan kuncinya. Tidak ada biaya untuk menggunakan kunci AWS yang dimiliki dan mereka tidak dihitung terhadap AWS KMS kuota untuk akun AWS.

- **AWS KMS kunci yang dikelola pelanggan** — Kunci yang dikelola pelanggan adalah kunci KMS di akun AWS yang Anda buat, miliki, dan kelola.

Anda memiliki kontrol penuh atas kunci KMS ini. Kunci yang dikelola pelanggan dikenakan biaya bulanan. Mereka juga dikenakan biaya untuk setiap permintaan API untuk AWS KMS melampaui tingkat gratis. Untuk informasi selengkapnya tentang AWS KMS harga, lihat [AWS Key Management Service harga](#).

Jenis kunci enkripsi tidak dapat diubah setelah Anda menyelesaikan penyiapan. Untuk informasi selengkapnya tentang AWS KMS dan jenis kunci enkripsi, lihat [AWS KMS dokumentasi](#).

Memilih jenis kunci enkripsi yang berbeda

1. Pilih tombol AWS KMS yang berbeda (lanjutan).

2. Pilih AWS KMS kunci atau masukkan nomor sumber daya Amazon (ARN).
3. Pilih Buat AWS KMS kunci.

## Konfigurasi Tanda

Tag bertindak sebagai label untuk mengatur sumber daya Nimble Studio Anda. Anda dapat menambahkan hingga 50 tanda untuk mengidentifikasi, mengatur, memfilter, dan mencari sumber daya.

Setiap tag terdiri dari dua bagian, yang Anda tentukan: tag Key dan tag opsional Value — misalnya, key: domain dan value:anycorpanystudio.com.

Anda dapat menambahkan atau menghapus tanda setelah Anda menyelesaikan pengaturan, kapan saja. Untuk informasi selengkapnya tentang tanda, lihat [Tanda di AWS sumber daya](#).

Untuk menambahkan tanda ke sumber daya

1. Pilih Tambahkan tanda baru.
2. Masukkan tanda Kunci.
3. (Opsional) Masukkan Nilai tag.

# Menghapus hapus hapus hapus hapus hapus hapus Studio

Jika Anda tidak lagi memerlukan Studio, Anda dapat menghapusnya. Ketika Anda menghapus studio Anda, hanya infrastruktur studio dihapus. AWSSumber daya Anda yang lain, seperti peran pengguna, kebijakan, dan data aplikasi tetap utuh.

## Important

Anda tidak dapat memulihkan setelah menghapusnya.

Untuk menghapus studio

1. Masuk ke AWS Management Console dan buka konsol [Nimble Studio](#).
2. Pilih Ringkasan studio.
3. Pilih Tindakan, lalu pilih Hapus studio.
4. Masukkand~~e~~lete, lalu pilih Hapus.

# Keamanan di Amazon Nimble Studio

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

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

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

## Important

Sangat disarankan agar Anda membaca dan membiasakan diri dengan [Pilar Keamanan - Kerangka AWS Well-Architected](#). Artikel ini berisi prinsip-prinsip kunci untuk mengamankan AWS infrastruktur Anda.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama ketika menggunakan Nimble Studio. Topik berikut menunjukkan cara mengonfigurasi Nimble Studio untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan Nimble Studio sumber daya Anda.

## Informasi Selengkapnya

- [Pilar Keamanan - Kerangka AWS Well-Architected](#)
- [Keamanan untuk AWS Cloud Development Kit \(AWS CDK\) \(AWS CDK\)](#)
- [Keamanan di Amazon Virtual Private Cloud](#)

- [AWS kredensial keamanan](#)
- Keamanan dalam Amazon EC2
  - [Linux](#)
  - [Windows](#)

## Mengatur Akun AWS keamanan

Panduan ini menunjukkan cara mengatur Akun AWS agar Anda menerima pemberitahuan saat sumber daya Anda disusupi, dan untuk memungkinkan Akun AWS pengguna tertentu mengaksesnya. Untuk mengamankan Akun AWS dan melacak sumber daya Anda, selesaikan langkah-langkah berikut.

### Daftar Isi

- [Hapus kunci akses akun Anda](#)
- [Mengaktifkan autentikasi multi-faktor](#)
- [Aktifkan CloudTrail di semua Wilayah AWS](#)
- [Siapkan Amazon GuardDuty dan notifikasi](#)

## Hapus kunci akses akun Anda

Anda dapat mengizinkan akses terprogram ke AWS sumber daya Anda dari AWS Command Line Interface (AWS CLI) atau dengan AWS API. Namun, AWS menyarankan agar Anda tidak membuat atau menggunakan kunci akses yang terkait dengan akun root Anda untuk akses terprogram.

Jika Anda masih memiliki kunci akses, kami sarankan Anda menghapusnya dan membuat pengguna. Kemudian, berikan pengguna itu hanya izin yang diperlukan untuk API yang Anda rencanakan untuk dipanggil. Anda dapat menggunakan pengguna tersebut untuk mengeluarkan kunci akses.

Untuk informasi selengkapnya, lihat [Mengelola Kunci Akses untuk Anda Akun AWS](#) di Referensi Umum AWS panduan.

## Mengaktifkan autentikasi multi-faktor

[Multi-factor authentication](#) (MFA) adalah kemampuan keamanan yang menyediakan lapisan otentikasi selain nama pengguna dan kata sandi Anda.

MFA bekerja seperti ini: Setelah Anda masuk dengan nama pengguna dan kata sandi Anda, Anda juga harus memberikan informasi tambahan yang hanya Anda yang memiliki akses fisik. Informasi ini dapat berasal dari perangkat keras MFA khusus, atau dari aplikasi di ponsel.

Anda harus memilih jenis perangkat MFA yang ingin Anda gunakan dari [daftar perangkat MFA yang didukung](#). Untuk perangkat keras, simpan perangkat MFA di lokasi yang aman.

Jika Anda menggunakan perangkat MFA virtual (seperti aplikasi telepon), pikirkan apa yang mungkin terjadi jika ponsel Anda hilang atau rusak. Salah satu pendekatannya adalah menjaga perangkat MFA virtual yang Anda gunakan di tempat yang aman. Pilihan lain adalah mengaktifkan lebih dari satu perangkat secara bersamaan, atau menggunakan opsi MFA virtual untuk pemulihan kunci perangkat.

Untuk mempelajari lebih lanjut tentang MFA, lihat [Mengaktifkan Perangkat Virtual Multi-Factor Authentication \(MFA\)](#).

## Sumber daya terkait

- [Memulai dengan Otentikasi Multi-Faktor](#)
- [Mengamankan Akses AWS Menggunakan MFA](#)

## Aktifkan CloudTrail di semua Wilayah AWS

Anda dapat melacak semua aktivitas di AWS sumber daya Anda dengan menggunakan [AWS CloudTrail](#). Kami menyarankan Anda menghidupkan CloudTrail sekarang. Ini dapat membantu AWS Support dan arsitek AWS solusi Anda memecahkan masalah keamanan atau konfigurasi, nanti.

Untuk mengaktifkan CloudTrail masuk semua Wilayah AWS, lihat [AWS CloudTrail Memperbarui — Aktifkan di Semua Wilayah dan Gunakan Beberapa Jalur](#).

Untuk mempelajari selengkapnya CloudTrail, lihat [Aktifkan Aktivitas API CloudTrail Log di Aktivitas Anda Akun AWS](#). Untuk mempelajari cara CloudTrail memonitor Nimble Studio, lihat [Logging panggilan Nimble Studio menggunakan AWS CloudTrail](#)

## Siapkan Amazon GuardDuty dan notifikasi

Amazon GuardDuty adalah layanan pemantauan keamanan berkelanjutan yang menganalisis dan memproses hal-hal berikut:

- [Sumber data](#)
- Log Aliran VPC Amazon
- AWS CloudTrail log acara manajemen
- CloudTrail Log peristiwa data S3
- Log DNS

Amazon GuardDuty mengidentifikasi aktivitas yang tidak terduga dan berpotensi tidak sah dan berbahaya dalam lingkungan Anda AWS . Aktivitas berbahaya dapat mencakup masalah seperti eskalasi hak istimewa, penggunaan kredensial yang terbuka, atau komunikasi dengan alamat IP atau domain berbahaya. Untuk mengidentifikasi aktivitas ini, GuardDuty gunakan umpan intelijen ancaman, seperti daftar alamat IP dan domain berbahaya, dan pembelajaran mesin. Misalnya, GuardDuty dapat mendeteksi instans Amazon EC2 yang disusupi yang melayani malware atau menambang bitcoin.

GuardDuty juga memantau perilaku Akun AWS akses untuk tanda-tanda kompromi. Ini termasuk penerapan infrastruktur yang tidak sah, seperti instance yang diterapkan di sebuah Wilayah AWS yang belum pernah digunakan. Ini juga mencakup panggilan API yang tidak biasa, seperti perubahan kebijakan kata sandi untuk mengurangi kekuatan kata sandi.

GuardDuty memberi tahu Anda tentang status AWS lingkungan Anda dengan menghasilkan [temuan keamanan](#). Anda dapat melihat temuan ini di GuardDuty konsol atau melalui [CloudWatch acara Amazon](#).

## Siapkan topik dan titik akhir Amazon SNS

Ikuti petunjuk dalam [Setup an Amazon SNS topik dan endpoint](#) tutorial.

## Siapkan EventBridge acara untuk GuardDuty temuan

Buat aturan EventBridge untuk mengirim acara untuk semua temuan yang GuardDuty dihasilkan.

Untuk membuat EventBridge acara untuk GuardDuty temuan

1. Masuk ke EventBridge konsol Amazon: <https://console.aws.amazon.com/events/>
2. Di panel navigasi, pilih Aturan. Kemudian, pilih Buat aturan.
3. Masukkan Nama dan Deskripsi untuk aturan baru. Lalu pilih Selanjutnya.
4. Biarkan AWS acara atau acara EventBridge mitra dipilih untuk sumber Acara.



5. Dalam pola Event, pilih AWS layanan untuk sumber Event. Kemudian GuardDuty untuk AWS layanan, dan GuardDuty Finding untuk jenis Event. Ini adalah topik yang Anda buat [Siapkan topik dan titik akhir Amazon SNS](#).
6. Pilih Selanjutnya.
7. Untuk Target 1, pilih AWS layanan. Pilih topik SNS di menu tarik-turun Pilih target. Kemudian pilih topik GuardDuty\_to\_email Anda.
8. Di bagian Pengaturan tambahan: Gunakan menu tarik-turun Konfigurasi input target untuk memilih Transformator input. Pilih Konfigurasi transformator input.
9. Masukkan kode berikut ke dalam bidang jalur Input di bagian Transformator input target.

```
{
  "severity": "$.detail.severity",
  "Account_ID": "$.detail.accountId",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

10. Untuk memformat email, masukkan kode berikut ke dalam bidang Template.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
in the <region> region."
"Finding Description:"
"<Finding_description>."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. Pilih Buat. Lalu pilih Selanjutnya.
12. (Opsional) Tambahkan tag jika Anda menggunakan tag untuk melacak AWS sumber daya Anda.
13. Pilih Selanjutnya.
14. Tinjau aturan Anda. Kemudian, pilih Buat aturan.

Setelah mengatur Akun AWS keamanan, Anda dapat memberikan akses ke pengguna tertentu dan menerima pemberitahuan saat sumber daya Anda disusupi.

# Perlindungan data di Amazon Nimble Studio

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon Nimble Studio. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS .

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

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-2](#).

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

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

[Model tanggung jawab AWS bersama](#) berlaku untuk perlindungan data di Amazon Nimble Studio. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk menjaga kontrol atas konten Anda yang di-host di infrastruktur ini. Konten ini mencakup konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan.

Untuk informasi selengkapnya tentang privasi data, silakan lihat [Pertanyaan Umum Privasi Data](#). Untuk informasi tentang perlindungan data di Uni Eropa, kunjungi [Pusat GDPR](#).

## Enkripsi diam

[Nimble Studio melindungi data studio sensitif dengan mengenkripsinya saat istirahat menggunakan kunci enkripsi yang disimpan di \(.AWS Key Management Service\) AWS KMS](#) Enkripsi saat istirahat tersedia di semua Wilayah AWS tempat Nimble Studio tersedia. Data studio yang kami enkripsi mencakup nama dan deskripsi semua jenis sumber daya, serta skrip komponen studio, parameter skrip, titik pemasangan, nama berbagi, dan data lainnya.

Mengenkripsi data berarti bahwa data sensitif yang disimpan pada disk tidak dapat dibaca oleh pengguna atau aplikasi mana pun tanpa kunci yang valid. Data terenkripsi dapat disimpan dengan aman saat istirahat dan hanya dapat didekripsi oleh pihak yang memiliki akses resmi ke kunci yang dikelola.

Untuk informasi tentang cara Nimble Studio menggunakan AWS KMS untuk mengenkripsi data saat istirahat, lihat [Manajemen kunci untuk Amazon Nimble Studio](#)

## Menggunakan hibah dengan kunci AWS KMS

Hibah adalah instrumen kebijakan yang memungkinkan [AWS prinsipal](#) untuk menggunakan AWS KMS kunci dalam operasi kriptografi. Hal ini juga dapat membiarkan mereka melihat kunci KMS dengan perintah `DescribeKey`, dan membuat dan mengelola hibah.

Hibah biasanya digunakan oleh Layanan AWS yang mengintegrasikan dengan AWS KMS untuk mengenkripsi data Anda saat istirahat. Layanan akan membuat pemberian izin atas nama pengguna di akun, menggunakan izinnya, dan menghentikan pemberian izin begitu tugasnya selesai.

Saat Nimble Studio membuat studio Anda, kami menyediakan dua peran untuk pengguna portal Nimble Studio: peran pengguna dan admin. Nimble Studio membuat hibah pada kunci yang dikelola pelanggan untuk peran ini untuk memberi mereka akses ke data terenkripsi studio.

**⚠ Important**

Jika Anda menghapus hibah, portal Nimble Studio tidak akan dapat digunakan untuk pengguna, hingga admin membuat hibah baru.

Untuk detail tentang cara Layanan AWS menggunakan hibah, lihat [Cara Layanan AWS menggunakan AWS KMS atau topik Enkripsi saat istirahat](#) di panduan pengguna atau panduan pengembang layanan.

## Enkripsi bergerak

Tabel berikut memberikan informasi tentang bagaimana data dienkripsi dalam perjalanan. Jika berlaku, metode perlindungan data lainnya untuk Nimble Studio juga dicantumkan.

Data	Jalur jaringan	Perlindungan
Aset web seperti gambar dan JavaScript file	Jalur jaringan adalah antara pengguna Nimble Studio dan Nimble Studio.	Enkripsi data menggunakan TLS 1.2 atau yang lebih baru.
Pixel dan lalu lintas streaming terkait	Jalur jaringan adalah antara pengguna Nimble Studio dan Nimble Studio.	Dienkripsi menggunakan 256-bit Advanced Encryption Standard (AES-256), dan diangkut menggunakan TLS 1.2 atau yang lebih baru.
Lalu lintas API	Jalannya adalah antara pengguna Nimble Studio dan Nimble Studio.	Dienkripsi menggunakan TLS 1.2 atau yang lebih baru. Permintaan untuk membuat koneksi ditandatangani menggunakan SiGv4.

## Manajemen kunci untuk Amazon Nimble Studio

Saat membuat studio baru, Anda dapat memilih salah satu kunci berikut untuk mengenkripsi data studio Anda:

- AWS kunci KMS yang dimiliki — Jenis enkripsi default. Kuncinya dimiliki oleh Nimble Studio (tanpa biaya tambahan).
- Kunci KMS yang dikelola pelanggan — Kunci disimpan di akun Anda dan dibuat, dimiliki, dan dikelola oleh Anda. Anda memiliki kendali penuh atas kunci. AWS KMS dikenakan biaya.

Menghapus kunci KMS yang dikelola pelanggan di AWS Key Management Service (AWS KMS) bersifat merusak dan berpotensi berbahaya. Ini secara permanen menghapus materi kunci dan semua metadata yang terkait dengan kunci. Setelah kunci KMS yang dikelola pelanggan dihapus, Anda tidak dapat lagi mendekripsi data yang dienkripsi oleh kunci itu. Ini berarti bahwa data menjadi tidak dapat dipulihkan.

Inilah sebabnya mengapa AWS KMS memberi pelanggan masa tunggu hingga 30 hari sebelum menghapus kunci. Masa tunggu default adalah 30 hari.

## Tentang masa tunggu

Karena merusak dan berpotensi berbahaya untuk menghapus kunci KMS yang dikelola pelanggan, kami meminta Anda untuk menetapkan masa tunggu 7 - 30 hari. Masa tunggu default adalah 30 hari.

Namun, masa tunggu sebenarnya mungkin hingga 24 jam lebih lama dari yang Anda jadwalkan. Untuk mendapatkan tanggal dan waktu aktual ketika kunci akan dihapus, gunakan [DescribeKey](#) operasi. Anda juga dapat melihat tanggal penghapusan kunci yang dijadwalkan di [AWS KMS konsol](#) pada halaman detail kunci, di bagian Konfigurasi umum. Perhatikan zona waktu.

Selama masa tunggu, status dan status kunci yang dikelola pelanggan adalah Penghapusan tertunda.

- [Kunci KMS yang dikelola pelanggan yang menunggu penghapusan tidak dapat digunakan dalam operasi kriptografi apa pun.](#)
- AWS KMS tidak [memutar kunci dukungan kunci](#) terkelola AWS KMS pelanggan yang sedang menunggu penghapusan.

Untuk informasi selengkapnya tentang menghapus kunci terkelola pelanggan, lihat [Menghapus AWS KMS kunci master pelanggan](#).

## Langkah-langkah keamanan data

Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi Akun AWS kredensial dan menyiapkan akun individual dengan 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 merekomendasikan TLS 1.2 atau versi yang lebih baru.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- 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 menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif, seperti nomor akun pelanggan, ke dalam bidang bentuk bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon Nimble Studio atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke Amazon Nimble Studio atau layanan lain mungkin diambil untuk dimasukkan dalam log diagnostik. Saat Anda memberikan URL ke server eksternal, jangan sertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

## Data diagnostik dan metrik

Selama penerapan dan penghapusan, StudioBuilder Amazon Nimble Studio mengumpulkan metrik tertentu yang kami gunakan untuk mendiagnosis masalah dan meningkatkan fitur dan pengalaman pengguna Nimble Studio.

### Jenis metrik yang dikumpulkan

- Informasi penggunaan – Perintah generik dan subperintah yang dijalankan.
- Kesalahan dan informasi diagnostik — Status dan durasi perintah yang dijalankan, termasuk kode keluar, nama pengecualian internal, dan kegagalan.
- Informasi sistem dan lingkungan — Versi Python, sistem operasi (Windows, Linux, atau macOS), dan lingkungan di mana StudioBuilder dijalankan.

# Identity and Access Management untuk Amazon Nimble Studio

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

## Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Amazon Nimble Studio bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Amazon Nimble Studio](#)
- [AWS kebijakan terkelola untuk Amazon Nimble Studio](#)
- [Pencegahan confused deputy lintas layanan](#)
- [Memecahkan masalah identitas dan akses Amazon Nimble Studio](#)

## Audiens

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

Pengguna layanan — Jika Anda menggunakan layanan Nimble Studio untuk melakukan pekerjaan Anda, maka Anda adalah pengguna layanan. Dalam hal ini, administrator Anda akan memberi Anda kredensi dan izin yang Anda perlukan untuk mengakses sumber daya yang Anda tetapkan. Saat Anda menggunakan lebih banyak fitur Nimble Studio untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Nimble Studio, lihat [Memecahkan masalah identitas dan akses Amazon Nimble Studio](#)

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Nimble Studio di perusahaan Anda, Anda mungkin memiliki akses penuh ke Nimble Studio. Tugas Anda adalah menentukan fitur dan sumber daya Nimble Studio mana yang harus diakses karyawan Anda. Kemudian, kirimkan permintaan ke administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih

lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Nimble Studio, lihat [Bagaimana Amazon Nimble Studio bekerja dengan IAM](#)

## Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensial identitas Anda. Untuk informasi selengkapnya tentang masuk menggunakan AWS Management Console, lihat [Masuk ke pengguna IAM atau pengguna root AWS Management Console sebagai IAM di Panduan Pengguna IAM](#).

Anda harus diautentikasi (masuk ke AWS) sebagai pengguna Akun AWS root, pengguna, atau dengan mengasumsikan peran IAM. Anda juga dapat menggunakan otentikasi masuk tunggal perusahaan Anda atau bahkan masuk menggunakan Google atau Facebook. Dalam kasus ini, administrator Anda sebelumnya telah menyiapkan federasi identitas menggunakan IAM role. Ketika Anda mengakses AWS menggunakan kredensi dari perusahaan lain, Anda mengambil peran secara tidak langsung.

Untuk masuk langsung ke [AWS Management Console](#), gunakan kata sandi Anda dengan alamat email pengguna root atau nama pengguna Anda. Anda dapat mengakses AWS secara terprogram menggunakan kunci akses pengguna root atau pengguna Anda.

AWS menyediakan SDK dan alat baris perintah untuk menandatangani permintaan Anda secara kriptografis menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, tandatangani permintaan sendiri. Lakukan ini menggunakan Versi Tanda Tangan 4, sebuah protokol untuk mengautentikasi permintaan API masuk. Untuk informasi selengkapnya tentang mengautentikasi permintaan, lihat [proses penandatanganan Versi Tanda Tangan 4](#) di Referensi Umum AWS

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat [Menggunakan otentikasi multi-faktor \(MFA\) AWS di Panduan Pengguna IAM](#).

### Akun AWS pengguna root

Saat pertama kali membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda, bahkan yang administratif. Sebagai gantinya, patuhi [praktik terbaik](#)



[dalam menggunakan pengguna root saja untuk membuat pengguna IAM pertama Anda](#). Kemudian, kunci kredensial pengguna akar dengan aman dan gunakan kredensial itu untuk melakukan beberapa tugas manajemen akun dan layanan saja.

## Pengguna dan grup

[Pengguna](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Seorang pengguna dapat memiliki kredensi jangka panjang atau satu set kunci akses. Untuk mempelajari cara membuat kunci akses, lihat [Mengelola kunci akses untuk pengguna IAM](#) di Panduan Pengguna IAM. Saat Anda membuat kunci akses untuk pengguna, lihat dan simpan key pair dengan aman. Anda tidak dapat memulihkan kunci akses rahasia di masa depan. Sebagai gantinya, buat access key pair baru.

[Grup IAM](#) adalah identitas yang menentukan kumpulan pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

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

## Peran IAM

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

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Izin pengguna sementara – Pengguna dapat mengambil peran IAM untuk mendapatkan izin yang berbeda sementara waktu agar dapat melakukan tugas tertentu.
- Akses pengguna federasi — Alih-alih membuat pengguna, Anda dapat menggunakan identitas yang ada dari AWS Directory Service, direktori pengguna perusahaan Anda, atau penyedia

identitas web. Ini dikenal sebagai pengguna gabungan. AWS menugaskan peran kepada pengguna gabungan saat akses diminta melalui [penyedia identitas](#). Untuk informasi selengkapnya tentang pengguna federasi, lihat [Pengguna dan peran gabungan](#) di Panduan Pengguna IAM.

- Keanggotaan — Nimble Studio menggunakan konsep yang disebut 'keanggotaan' untuk memberikan akses pengguna ke profil peluncuran tertentu. Keanggotaan memungkinkan administrator studio untuk mendelegasikan akses sumber daya ke pengguna, tanpa harus menulis, atau memahami, kebijakan IAM. Saat administrator Nimble Studio membuat keanggotaan untuk pengguna di profil peluncuran, pengguna diberi wewenang untuk melakukan tindakan IAM yang diperlukan untuk menggunakan profil peluncuran, seperti melihat propertinya dan memulai sesi streaming menggunakan profil peluncuran tersebut.
- Peran layanan – Peran layanan adalah [peran IAM](#) yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Peran layanan hanya menyediakan akses dalam akun Anda dan tidak dapat digunakan untuk memberikan akses ke layanan di akun lain. Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan](#) Pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Nimble Studio tidak mendukung peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 di](#) Panduan Pengguna IAM.

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

## Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya IAM. AWS Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. Anda dapat masuk sebagai pengguna root atau pengguna,

atau Anda dapat mengambil peran IAM. Saat Anda kemudian membuat permintaan, AWS evaluasi kebijakan berbasis identitas atau berbasis sumber daya terkait. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat [Ringkasan kebijakan JSON di Panduan Pengguna IAM](#).

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

Setiap entitas IAM (pengguna atau peran) dimulai tanpa izin. Dengan kata lain, secara default, pengguna tidak dapat melakukan apa pun, termasuk mengubah kata sandi mereka sendiri. Untuk memberikan izin kepada pengguna untuk melakukan sesuatu, administrator harus melampirkan kebijakan izin kepada pengguna. Atau administrator dapat menambahkan pengguna ke grup yang memiliki izin yang dimaksudkan. Ketika administrator memberikan izin untuk grup, semua pengguna dalam grup tersebut akan diberi izin tersebut.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

## Kebijakan berbasis identitas

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

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

## Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan

kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya di mana kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya itu dan untuk kondisi apa. [Tentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

## Daftar kontrol akses (ACL) di Nimble Studio

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat [Gambaran umum daftar kontrol akses \(ACL\)](#) dalam Panduan Developer Amazon Simple Storage Service.

## Jenis-jenis kebijakan lain

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

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

anggota, termasuk setiap pengguna Akun AWS root. Untuk informasi selengkapnya tentang Organizations dan SCP, lihat [Cara kerja SCP](#) di AWS Organizations Panduan Pengguna.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah persimpangan kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) di Panduan Pengguna IAM.

## Berbagai jenis kebijakan

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

## Bagaimana Amazon Nimble Studio bekerja dengan IAM

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

Fitur IAM yang dapat Anda gunakan dengan Amazon Nimble Studio

Fitur IAM	Dukungan Studio gesit
<a href="#">Tindakan kebijakan untuk Nimble Studio</a>	Ya
<a href="#">Sumber daya kebijakan untuk Nimble Studio</a>	Ya
<a href="#">Kunci kondisi kebijakan untuk Nimble Studio</a>	Ya
<a href="#">Daftar kontrol akses (ACL) di Nimble Studio</a>	Tidak
<a href="#">Kontrol akses berbasis atribut (ABAC) dengan Nimble Studio</a>	Ya
<a href="#">Menggunakan kredensial sementara dengan Nimble Studio</a>	Ya
<a href="#">Izin utama lintas layanan untuk Nimble Studio</a>	Ya

Fitur IAM	Dukungan Studio gesit
<a href="#">Peran layanan untuk Nimble Studio</a>	Ya
<a href="#">Peran terkait layanan untuk Nimble Studio</a>	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara Layanan AWS kerja Nimble Studio dan lainnya dengan sebagian besar fitur IAM, lihat [Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM](#).

## Kebijakan berbasis identitas untuk Nimble Studio

Mendukung kebijakan berbasis identitas	Ya
--	----

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

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi tindakan yang diizinkan atau ditolak. Anda tidak dapat menentukan prinsipal dalam kebijakan berbasis identitas karena berlaku untuk pengguna atau peran yang dilampirkan. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [referensi elemen kebijakan IAM JSON](#) di Panduan Pengguna IAM.

### Contoh kebijakan berbasis identitas untuk Amazon Nimble Studio

Untuk melihat contoh kebijakan berbasis identitas Nimble Studio, lihat. [Contoh kebijakan berbasis identitas untuk Amazon Nimble Studio](#)

## Kebijakan berbasis sumber daya dalam Nimble Studio

Mendukung kebijakan berbasis sumber daya	Tidak
--	-------

Nimble Studio tidak mendukung kebijakan berbasis sumber daya atau akses lintas akun. Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya.

Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya di mana kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya itu dan untuk kondisi apa. [Tentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau Layanan AWS

## Tindakan kebijakan untuk Nimble Studio

Mendukung tindakan kebijakan

Ya

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

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

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

Untuk melihat daftar tindakan Nimble Studio, lihat [Tindakan yang ditentukan oleh Amazon Nimble Studio](#) di Referensi Otorisasi Layanan.

Tindakan kebijakan di Nimble Studio menggunakan awalan berikut sebelum tindakan:

```
nimble
```

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

```
"Action": [  
    "nimble:action1",
```

```
"nimble:action2"  
]
```

Untuk melihat contoh kebijakan berbasis identitas Nimble Studio, lihat. [Contoh kebijakan berbasis identitas untuk Amazon Nimble Studio](#)

## Sumber daya kebijakan untuk Nimble Studio

Mendukung sumber daya kebijakan Ya

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

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

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

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

Untuk melihat contoh kebijakan berbasis identitas Nimble Studio, lihat. [Contoh kebijakan berbasis identitas untuk Amazon Nimble Studio](#)

## Kunci kondisi kebijakan untuk Nimble Studio

Mendukung kunci syarat kebijakan Ya

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



ConditionElement (atau Condition **block**) lets you specify conditions in which a statement is in effect. The `Condition` elemen adalah opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

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

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

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi global AWS, lihat [Kunci konteks kondisi global AWS](#) dalam Panduan Pengguna IAM.

Untuk melihat contoh kebijakan berbasis identitas Nimble Studio, lihat. [Contoh kebijakan berbasis identitas untuk Amazon Nimble Studio](#)

## Daftar kontrol akses (ACL) di Nimble Studio

Mendukung ACL

Tidak

Nimble Studio tidak mendukung daftar kontrol akses (ACL). ACL mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

## Kontrol akses berbasis atribut (ABAC) dengan Nimble Studio

Mendukung ABAC (tanda dalam kebijakan)

Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna

atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang kebijakan ABAC untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

Untuk mengontrol akses berdasarkan tandanya, Anda memberikan informasi tanda di [elemen syarat](#) kebijakan dengan menggunakan kunci syarat `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Untuk informasi lebih lanjut tentang ABAC, lihat [Apa itu ABAC?](#) di Panduan Pengguna IAM. Untuk melihat tutorial dengan langkah-langkah untuk menyiapkan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\) di Panduan Pengguna IAM](#).

## Menggunakan kredensial sementara dengan Nimble Studio

Mendukung penggunaan kredensial sementara    Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensial sementara, lihat [Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM](#).

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

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

## Izin utama lintas layanan untuk Nimble Studio

Mendukung izin pengguna utama    Ya

## Peran layanan untuk Nimble Studio

Mendukung peran layanan

Ya

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Peran layanan hanya menyediakan akses dalam akun Anda dan tidak dapat digunakan untuk memberikan akses ke layanan di akun lain. Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan Pengguna IAM](#).

### Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas Nimble Studio. Edit peran layanan hanya jika Nimble Studio memberikan panduan untuk melakukannya.

## Peran terkait layanan untuk Nimble Studio

Mendukung peran terkait layanan

Tidak

Nimble Studio tidak mendukung peran terkait layanan. Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat menggunakan peran untuk melakukan tindakan atas nama Anda. Peran tertaut layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat [Layanan AWS bahwa bekerja dengan IAM](#). Cari layanan dalam tabel yang memiliki Yes di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

## Contoh kebijakan berbasis identitas untuk Amazon Nimble Studio

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Nimble Studio. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. Administrator harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan tindakan pada sumber daya yang mereka

butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna atau grup yang memerlukan izin tersebut.

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

## Topik

- [Praktik terbaik kebijakan](#)

## Praktik terbaik kebijakan

Kebijakan berbasis identitas adalah pilihan yang sangat tepat. Mereka menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Nimble Studio di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulai menggunakan kebijakan AWS terkelola — Untuk mulai menggunakan Nimble Studio dengan cepat, gunakan kebijakan AWS terkelola untuk memberi karyawan Anda izin yang mereka butuhkan. Kebijakan ini sudah tersedia di akun Anda dan dikelola, serta diperbarui oleh AWS. Untuk informasi selengkapnya, lihat [Memulai menggunakan izin dengan kebijakan AWS terkelola](#) di Panduan Pengguna IAM.
- Pemberian hak istimewa terendah – Ketika Anda membuat kebijakan kustom, berikan izin yang diperlukan saja untuk melakukan tugas. Mulai dengan satu set izin minimum dan berikan izin tambahan sesuai kebutuhan. Melakukan hal tersebut lebih aman daripada memulai dengan izin yang terlalu fleksibel, lalu mencoba memperketatnya nanti. Untuk informasi selengkapnya, lihat [Pemberian hak istimewa terendah](#) dalam Panduan Pengguna IAM.
- Aktifkan MFA untuk operasi sensitif — Untuk keamanan ekstra, pengguna harus menggunakan otentikasi multi-faktor (MFA) untuk mengakses sumber daya sensitif atau operasi API. Untuk informasi selengkapnya, lihat [Menggunakan otentikasi multi-faktor \(MFA\) AWS di Panduan Pengguna IAM](#).
- Gunakan ketentuan kebijakan untuk keamanan ekstra — Sejauh praktis, tentukan kondisi yang memungkinkan kebijakan berbasis identitas Anda mengakses sumber daya. Misalnya, Anda dapat menulis persyaratan untuk menentukan jangkauan alamat IP yang diizinkan untuk mengajukan permintaan. Anda juga dapat menulis persyaratan untuk mengizinkan permintaan hanya dalam rentang tanggal atau waktu tertentu, atau untuk mewajibkan penggunaan SSL atau autentikasi multifaktor (MFA). Untuk informasi selengkapnya, lihat [elemen kebijakan IAM JSON: Kondisi](#) dalam Panduan Pengguna IAM.

## AWS kebijakan terkelola untuk Amazon Nimble Studio

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

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

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

Pengguna akhir Anda akan mengakses Amazon Nimble Studio terutama menggunakan portal Nimble Studio. Saat membuat studio Anda menggunakan StudioBuilder atau konsol Nimble Studio, satu peran IAM dibuat untuk setiap persona studio: administrator studio dan pengguna studio. Masing-masing memiliki masing-masing kebijakan terkelola IAM terlampir. Portal Nimble Studio memberikan pengalaman di mana pengguna hanya dapat membuat daftar dan menggunakan sumber daya yang mereka miliki izin untuk diakses.

Portal Nimble Studio memberikan pengalaman di mana pengguna hanya dapat membuat daftar dan menggunakan sumber daya yang mereka akses dan portal bergantung pada konten kebijakan ini untuk beroperasi dengan benar. Pengguna akhir Nimble Studio akan menggunakan portal untuk mengakses studio cloud mereka. Jadi, ketika admin membuat studio mereka menggunakan StudioBuilder, satu peran IAM dibuat untuk setiap orang yang perlu mengakses studio. Ini termasuk administrator studio dan pengguna studio, masing-masing dengan kebijakan terkelola IAM masing-masing terlampir.

Untuk daftar dan deskripsi kebijakan fungsi pekerjaan, lihat [kebijakan AWS terkelola untuk fungsi pekerjaan](#) di Panduan Pengguna IAM.

## AWS kebijakan terkelola: **AmazonNimbleStudio-LaunchProfileWorker**

Anda dapat melampirkan kebijakan [AmazonNimbleStudio-LaunchProfileWorker](#) ke identitas IAM Anda.

Lampirkan kebijakan ini ke instans EC2 yang dibuat oleh Nimble Studio Builder untuk memberikan akses ke sumber daya yang dibutuhkan oleh pekerja profil peluncuran Nimble Studio.

### Detail izin

Kebijakan ini mencakup izin berikut.

- ds - Memungkinkan LaunchProfile pekerja untuk menemukan informasi koneksi tentang yang AWS Managed Microsoft AD terkait dengan a LaunchProfile.
- ec2 - Memungkinkan LaunchProfile pekerja untuk menemukan kelompok keamanan dan informasi subnet untuk menghubungkan ke file. LaunchProfile
- fsx - Memungkinkan LaunchProfile pekerja menemukan informasi koneksi ke volume Amazon FSx yang terkait dengan file. LaunchProfile

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      },
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ]
}
```

```
    }
  ],
  "Version": "2012-10-17"
}
```

## AWS kebijakan terkelola: **AmazonNimbleStudio-StudioAdmin**

Anda dapat melampirkan kebijakan [AmazonNimbleStudio-StudioAdmin](#) ke identitas IAM Anda.

Lampirkan kebijakan ini ke peran Admin yang terkait dengan studio Anda untuk memberikan akses ke sumber daya Amazon Nimble Studio yang terkait dengan admin studio dan sumber daya studio terkait di layanan lain.

### Detail izin

Kebijakan ini mencakup izin berikut.

- `lincch` - Memungkinkan Pengguna Studio mengakses sumber daya Nimble yang telah didelegasikan kepada mereka oleh `StudioAdmins`
- `sso` - Memungkinkan Pengguna Studio kemampuan untuk melihat nama pengguna lain di studio.
- `identitystore` - Memungkinkan Pengguna Studio kemampuan untuk melihat nama pengguna lain di studio.
- `ds` - Memungkinkan Nimble Studio untuk menambahkan workstation virtual ke yang AWS Managed Microsoft AD terkait dengan studio.
- `ec2` - Memungkinkan Nimble Studio untuk melampirkan workstation virtual ke VPC Anda yang dikonfigurasi.
- `fsx` - Memungkinkan Nimble Studio menghubungkan workstation virtual ke volume Amazon FSx yang dikonfigurasi.
- `cloudwatch` - Memungkinkan Nimble Studio untuk mengambil metrik. `CloudWatch`

```
{
  "Statement": [
    {
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",

```

```

    "nimble:StopStreamingSession",
    "nimble:CreateStreamingSessionStream",
    "nimble:GetStreamingSessionStream",
    "nimble>DeleteStreamingSession",
    "nimble:ListStreamingSessionBackups",
    "nimble:GetStreamingSessionBackup",
    "nimble:ListEulas",
    "nimble:ListEulaAcceptances",
    "nimble:GetEula",
    "nimble:AcceptEulas",
    "nimble:ListStudioMembers",
    "nimble:GetStudioMember",
    "nimble:ListStreamingSessions",
    "nimble:GetStreamingImage",
    "nimble:ListStreamingImages",
    "nimble:GetLaunchProfileInitialization",
    "nimble:GetLaunchProfileDetails",
    "nimble:GetFeatureMap",
    "nimble:PutStudioLogEvents",
    "nimble:ListLaunchProfiles",
    "nimble:GetLaunchProfile",
    "nimble:GetLaunchProfileMember",
    "nimble:ListLaunchProfileMembers",
    "nimble:PutLaunchProfileMembers",
    "nimble:UpdateLaunchProfileMember",
    "nimble>DeleteLaunchProfileMember"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "sso-directory:DescribeUsers",
    "sso-directory:SearchUsers",
    "identitystore:DescribeUser",
    "identitystore:ListUsers"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [

```



```

    "ds:CreateComputer",
    "ds:DescribeDirectories",
    "ec2:DescribeSubnets",
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2>DeleteNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2:DescribeSecurityGroups",
    "fsx:DescribeFileSystems"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:CalledViaLast": "nimble.amazonaws.com"
    }
  }
},
{
  "Effect": "Allow",
  "Action": "cloudwatch:GetMetricData",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "cloudwatch:namespace": "AWS/NimbleStudio"
    }
  }
}
],
"Version": "2012-10-17"
}

```

## AWS kebijakan terkelola: **AmazonNimbleStudio-StudioUser**

Anda dapat melampirkan kebijakan [AmazonNimbleStudio-StudioUser](#) ke identitas IAM Anda.

Lampirkan kebijakan ini ke peran Pengguna yang terkait dengan studio Anda untuk memberikan akses ke sumber daya Amazon Nimble Studio yang terkait dengan pengguna studio dan sumber daya studio terkait di layanan lain.

### Detail izin

Kebijakan ini mencakup izin berikut.

- `linch` - Memungkinkan Pengguna Studio mengakses sumber daya Nimble yang telah didelegasikan kepada mereka oleh `StudioAdmins`
- `ss0` - Memungkinkan Pengguna Studio kemampuan untuk melihat nama pengguna lain di studio.
- `identitystore` - Memungkinkan Pengguna Studio kemampuan untuk melihat nama pengguna lain di studio.
- `ds` - Memungkinkan Nimble Studio untuk menambahkan workstation virtual ke yang AWS Managed Microsoft AD terkait dengan studio.
- `ec2` - Memungkinkan Nimble Studio untuk melampirkan workstation virtual ke VPC Anda yang dikonfigurasi.
- `fsx` - Memungkinkan Nimble Studio menghubungkan workstation virtual ke volume Amazon FSx yang dikonfigurasi.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": [
    "sso-directory:DescribeUsers",
    "sso-directory:SearchUsers",
    "identitystore:DescribeUser",
    "identitystore:ListUsers"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "nimble:ListLaunchProfiles"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "nimble:requesterPrincipalId": "${nimble:principalId}"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "nimble:ListStudioMembers",
    "nimble:GetStudioMember",
    "nimble:ListEulas",
    "nimble:ListEulaAcceptances",
    "nimble:GetFeatureMap",
    "nimble:PutStudioLogEvents"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "nimble:StartStreamingSession",
    "nimble:StopStreamingSession",
    "nimble>DeleteStreamingSession",
    "nimble:GetStreamingSession",
    "nimble>CreateStreamingSessionStream",
```

```

    "nimble:GetStreamingSessionStream",
    "nimble:ListStreamingSessions"
    "nimble:ListStreamingSessionBackups",
    "nimble:GetStreamingSessionBackup"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "nimble:ownedBy": "${nimble:requesterPrincipalId}"
    }
  }
}
],
"Version": "2012-10-17"
}

```

## Pembaruan Nimble Studio ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon Nimble Studio sejak layanan ini mulai melacak perubahan ini.

Perubahan	Deskripsi	Tanggal
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioUser</a> - Kebijakan yang diperbarui	Amazon Nimble Studio memperbarui kebijakan untuk menggunakan versi terbaru dari layanan Identity Store.	September 22, 2023
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioAdmin</a> - Kebijakan yang diperbarui	Amazon Nimble Studio memperbarui kebijakan untuk menggunakan versi terbaru dari layanan Identity Store.	September 22, 2023
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioUser</a> - Kebijakan yang diperbarui	Amazon Nimble Studio memperbarui kebijakan untuk memungkinkan pengguna studio melihat cadangan workstation mereka.	Desember 20, 2022

Perubahan	Deskripsi	Tanggal
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioAdmin</a> - Kebijakan yang diperbarui	Amazon Nimble Studio memperbarui kebijakan agar admin studio dapat melihat cadangan workstation mereka.	Desember 20, 2022
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioUser</a> - Kebijakan yang diperbarui	Amazon Nimble Studio memperbarui kebijakan agar admin studio dapat mengambil metrik. CloudWatch	11 November 2021
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioUser</a> - Kebijakan yang diperbarui	Amazon Nimble Studio memperbarui kebijakan untuk memungkinkan pengguna studio memulai dan menghentikan workstation mereka.	November 1, 2021
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioAdmin</a> - Kebijakan yang diperbarui	Amazon Nimble Studio memperbarui kebijakan untuk memungkinkan admin studio memulai dan menghentikan workstation mereka.	November 1, 2021
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioUser</a> - Kebijakan yang diperbarui	Amazon Nimble Studio memperbarui kebijakan untuk mengizinkan akses ke sumber daya sesi streaming berdasarkan kondisional, bukan. <code>nimble:ownedBy</code> <code>nimble:createdBy</code>	16 Agustus 2021

Perubahan	Deskripsi	Tanggal
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioUser</a> – Kebijakan baru	Amazon Nimble Studio menambahkan kebijakan baru yang memungkinkan akses ke sumber daya yang terkait dengan pengguna studio dan sumber daya studio terkait di layanan lain.	28 April 2021
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-StudioAdmin</a> - Kebijakan baru	Amazon Nimble Studio menambahkan kebijakan baru yang memungkinkan akses ke sumber daya yang terkait dengan admin studio dan sumber daya studio terkait di layanan lain.	28 April 2021
<a href="#">AWS kebijakan terkelola: AmazonNimbleStudio-LaunchProfileWorker</a> – Kebijakan baru	Amazon Nimble Studio menambahkan kebijakan baru yang memungkinkan akses ke sumber daya yang dibutuhkan oleh pekerja profil peluncuran Nimble Studio.	28 April 2021
Amazon Nimble Studio mulai melacak perubahan	Amazon Nimble Studio mulai melacak perubahan untuk kebijakan yang AWS dikelola.	28 April 2021

## Pencegahan confused deputy lintas layanan

Masalah deputy yang membingungkan adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak atas sumber daya pelanggan lain dengan cara yang

seharusnya tidak memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan pengguna utama layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan global dalam kebijakan sumber daya untuk membatasi izin yang diberikan Identity and Access Management (IAM) kepada Amazon Nimble Studio untuk mengakses sumber daya Anda. Jika Anda menggunakan kedua kunci konteks kondisi global, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menggunakan id akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Nilai `aws:SourceArn` harus ARN studio dan `aws:SourceAccount` harus id akun Anda. Anda tidak akan tahu apa id studio sampai studio dibuat karena dihasilkan oleh Nimble Studio. Setelah studio Anda dibuat, Anda dapat memperbarui kebijakan kepercayaan dengan id studio akhir yang ditetapkan sebagai `aws:SourceArn`.

Cara paling efektif untuk melindungi dari masalah confused deputy adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan wildcard (\*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:nimble::123456789012:*`.

Pengguna akhir Anda mengambil peran studio Anda saat mereka masuk ke portal Nimble Studio. Saat Anda membuat studio, AWS mengonfigurasi peran dan mengevaluasi kebijakan. AWS mengevaluasi kebijakan setiap kali salah satu pengguna Anda masuk ke portal Nimble Studio. Saat Anda membuat studio, Anda tidak dapat memodifikasi `aws:SourceArn`. Setelah Anda selesai membuat studio Anda, Anda dapat menggunakan StudioARN Anda untuk `aws:SourceArn`

Contoh berikut adalah kebijakan peran asumsi yang menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceArn` dan `aws:SourceAccount` global di Nimble Studio untuk mencegah masalah deputy yang membingungkan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
```

```
    },
    "Action": [
      "sts:AssumeRole",
      "sts:TagSession"
    ],
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "StringLike": {
        "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
      }
    }
  }
]
```

## Memecahkan masalah identitas dan akses Amazon Nimble Studio

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

### Topik

- [Saya tidak berwenang untuk melakukan aksi di Nimble Studio.](#)
- [Saya tidak berwenang untuk melakukan iam:PassRole.](#)
- [Saya ingin melihat kunci akses saya.](#)
- [Saya seorang administrator dan ingin mengizinkan orang lain mengakses Nimble Studio.](#)
- [Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Nimble Studio saya.](#)

### Saya tidak berwenang untuk melakukan aksi di Nimble Studio.

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

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



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

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

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

Saya tidak berwenang untuk melakukan iam:PassRole.

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan iam:PassRole tindakan, hubungi administrator Anda untuk mendapatkan bantuan. Minta mereka memperbarui kebijakan Anda agar Anda dapat meneruskan peran ke Nimble Studio.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan itu, alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukan ini, Anda memerlukan izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna bernama johndoe mencoba menggunakan konsol untuk melakukan tindakan di Nimble Studio. Namun, tindakan ini mengharuskan layanan memiliki izin yang diberikan oleh peran layanan. John tidak memiliki izin untuk meneruskan peran ke layanan.

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

Dalam hal ini, John meminta administratornya untuk memperbarui kebijakannya untuk memberikan izin untuk melakukan iam:PassRole tindakan tersebut.

Saya ingin melihat kunci akses saya.

Amazon Nimble Studio tidak menyediakan kunci akses. Untuk mempelajari kunci akses rahasia, lihat [Mengelola kunci akses di Panduan Pengguna IAM](#).

#### Important

Jangan berikan kunci akses Anda kepada pihak ketiga, bahkan untuk membantu [menemukan ID pengguna kanonik Anda](#). Dengan melakukan tindakan ini, Anda mungkin memberi seseorang akses permanen ke akun Anda.

Saat membuat access key pair, Anda akan diminta untuk menyimpan ID kunci akses dan kunci akses rahasia di lokasi yang aman. secret access key hanya tersedia saat Anda membuatnya. Jika Anda kehilangan kunci akses rahasia Anda, tambahkan kunci akses baru ke pengguna Anda. Anda dapat memiliki maksimum dua access key. Jika Anda sudah memiliki dua, hapus satu key pair sebelum membuat yang baru. Untuk melihat instruksi, lihat [Mengelola kunci akses](#) di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Nimble Studio.

Untuk memungkinkan orang lain mengakses Nimble Studio, buat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Mereka akan menggunakan kredensial untuk entitas tersebut untuk mengakses AWS. Kemudian, lampirkan kebijakan ke entitas yang memberi mereka izin yang benar.

Nimble Studio menyediakan Anda dengan AmazonNimbleStudio-StudioUser di AWS Management Console Admin TI yang mengelola Konsol menggunakan kebijakan ini untuk memberikan akses studio kepada orang lain.

Untuk tutorial tentang menggunakan kebijakan admin, lihat [Menyiapkan untuk Nimble Studio](#) panduannya. Untuk mempelajari cara melampirkan kebijakan yang ada ke pengguna, seperti kebijakan profil pengguna dan peluncuran, lihat [Membuat pengguna IAM \(konsol\)](#).

Untuk informasi tentang mengimpor kebijakan, lihat Membuat pengguna dan grup yang didelegasikan IAM pertama Anda di Panduan Pengguna [IAM](#).

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Nimble Studio saya.

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Nimble Studio mendukung fitur-fitur ini, lihat. [Bagaimana Amazon Nimble Studio bekerja dengan IAM](#)

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna yang diautentikasi secara eksternal \(federasi identitas\) di Panduan Pengguna IAM](#).
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, [lihat Perbedaan peran IAM dari kebijakan berbasis sumber daya di Panduan Pengguna IAM](#).

## Pencatatan dan pemantauan peristiwa keamanan dengan Nimble Studio

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon Nimble Studio dan solusi Anda AWS . Kumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi.

AWS [dan Nimble Studio menyediakan alat untuk memantau sumber daya Anda dan menanggapi potensi insiden, termasuk Logging panggilan Nimble Studio menggunakan AWS CloudTrail dan Panduan Pengguna.AWS CloudFormation](#)

Untuk informasi selengkapnya tentang cara kerja Amazon Nimble Studio AWS CloudFormation, termasuk contoh templat JSON dan YAMAL, lihat referensi [sumber daya dan properti Amazon Nimble Studio](#) di Panduan Pengguna. AWS CloudFormation Untuk memahami cara menggunakan CloudFormation templat, lihat [AWS CloudFormation konsep](#).

### Topik

- [Logging panggilan Nimble Studio menggunakan AWS CloudTrail](#)

## Logging panggilan Nimble Studio menggunakan AWS CloudTrail

Amazon Nimble Studio terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS di Nimble Studio. CloudTrail

menangkap semua panggilan API untuk Nimble Studio sebagai acara. Panggilan yang diambil termasuk panggilan dari konsol Nimble Studio dan panggilan kode ke operasi Amazon Nimble Studio.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Nimble Studio. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Nimble Studio, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

## Informasi Nimble Studio di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Nimble Studio, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa lain dalam sejarah Layanan AWS Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat Acara dengan Riwayat CloudTrail Acara](#).

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Nimble Studio, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi lainnya Layanan AWS untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log.

Untuk informasi selengkapnya, lihat berikut:

[Gambaran umum untuk membuat jejak](#)

[CloudTrail layanan dan integrasi yang didukung](#)

[Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)

[Menerima file CloudTrail log dari beberapa Wilayah](#)

[Menerima file CloudTrail log dari beberapa akun](#)

Tindakan Nimble Studio dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API [Amazon Nimble Studio](#). Misalnya, panggilan ke CreateStudio, GetStudio dan DeleteStudio tindakan menghasilkan entri dalam file CloudTrail log.

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

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

Untuk informasi selengkapnya, lihat [elemen Identitas CloudTrail pengguna](#).

## Memahami entri file log Nimble Studio

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

Contoh JSON ini menunjukkan tiga tindakan:

- TINDAKAN\_1: CreateStudio
- TINDAKAN\_2: GetStudio
- TINDAKAN\_3: DeleteStudio

```
{
  "eventVersion": "0",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
    "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-Session",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE-accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLE-PrincipalID",
```

```

        "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
        "accountId": "111122223333",
        "userName": "EXAMPLE-UserName"
    },
    "webIdFederationData": {},
    "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-03-08T23:25:49Z"
    }
}
},
"eventTime": "2021-03-08T23:25:49Z",
"eventSource": "nimble.amazonaws.com",
"eventName": "CreateStudio",
"awsRegion": "us-west-2",
"sourceIPAddress": "192.0.2.0",
"userAgent": "EXAMPLE-userAgent",
"requestParameters": {
    "displayName": "Studio Name",
    "studioName": "EXAMPLE-studioName",
    "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
    "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
},
"responseElements": {},
"requestID": "EXAMPLE-requestID",
"eventID": "EXAMPLE-eventID",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",

```

```

        "principalId": "EXAMPLE-PrincipalID",
        "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
        "accountId": "111122223333",
        "userName": "EXAMPLE-UserName"
    },
    "webIdFederationData": {},
    "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-03-08T23:44:25Z"
    }
}
},
"eventTime": "2021-03-08T23:44:25Z",
"eventSource": "nimble.amazonaws.com",
"eventName": "GetStudio",
"awsRegion": "us-west-2",
"sourceIPAddress": "192.0.2.0",
"userAgent": "EXAMPLE-userAgent",
"requestParameters": {
    "studioId": "us-west-2-EXAMPLE-studioId"
},
"responseElements": null,
"requestID": "EXAMPLE-requestID",
"eventID": "EXAMPLE-eventID",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",

```

```

        "accountId": "111122223333",
        "userName": "EXAMPLE-UserName"
    },
    "webIdFederationData": {},
    "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-03-08T23:45:14Z"
    }
}
},
"eventTime": "2021-03-08T23:44:14Z",
"eventSource": "nimble.amazonaws.com",
"eventName": "DeleteStudio",
"awsRegion": "us-west-2",
"sourceIPAddress": "192.0.2.0",
"userAgent": "EXAMPLE-userAgent",
"requestParameters": {
    "studioId": "us-west-2-EXAMPLE-studioId"
},
"responseElements": {
    "studio": {
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
        "displayName": "My New Studio Name",
        "homeRegion": "us-west-2",
        "ssoClientId": "EXAMPLE-ssoClientId",
        "state": "DELETING",
        "statusCode": "DELETING_STUDIO",
        "statusMessage": "Deleting studio",
        "studioEncryptionConfiguration": {
            "keyType": "AWS_OWNED_CMK"
        },
        "studioId": "us-west-2-EXAMPLE-studioId",
        "studioName": "EXAMPLE-studioName",
        "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
        "tags": {},
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
    }
},
"requestID": "EXAMPLE-requestID",
"eventID": "EXAMPLE-eventID",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,

```



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

Dalam contoh, Anda akan melihat bahwa peristiwa menunjukkan Wilayah, alamat IP, dan "RequestParameters" lainnya seperti "" dan userRoleArn "adminRoleArn" yang akan membantu Anda mengidentifikasi acara. Anda dapat melihat waktu dan tanggal di "creationDate", dan sumber tempat permintaan berasal, yang ditandai sebagai "EventSource": "nimble.amazonaws.com".

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di IAM atau AWS STS, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan Layanan AWS peristiwa lain dalam sejarah Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS.

AWS CloudTrail menangkap semua panggilan API untuk IAM dan AWS Security Token Service (AWS STS) sebagai peristiwa, termasuk panggilan dari konsol dan panggilan API. Untuk mempelajari lebih lanjut tentang penggunaan CloudTrail dengan IAM dan AWS STS, lihat [Logging panggilan IAM dan AWS STS API dengan](#). AWS CloudTrail

Untuk informasi selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Untuk informasi tentang layanan pemantauan lain yang ditawarkan Amazon, lihat [Panduan CloudWatch Pengguna Amazon](#).

## Validasi kepatuhan untuk Amazon Nimble Studio


Amazon Nimble Studio mengikuti [model tanggung jawab bersama](#), dan kepatuhan dibagi antara AWS dan pelanggan kami.

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

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#) .

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

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

 Note

Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat [Referensi Layanan yang Memenuhi Syarat HIPAA](#).

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

## Keamanan infrastruktur di Amazon Nimble Studio

Sebagai layanan terkelola, Amazon Nimble Studio dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Nimble Studio melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

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

## Praktik terbaik keamanan untuk Nimble Studio

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

## Pemantauan

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Nimble Studio dan solusi Anda AWS . Untuk informasi selengkapnya tentang memantau dan menanggapi peristiwa, lihat [Pencatatan dan pemantauan peristiwa keamanan dengan Nimble Studio](#).

## Perlindungan data

Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi Akun AWS kredensial dan menyiapkan akun individual dengan 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 merekomendasikan TLS 1.2 atau versi yang lebih baru.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data pribadi yang disimpan di Amazon Simple Storage Service (Amazon S3).
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi lebih lanjut tentang titik akhir FIPS yang tersedia, lihat [Standar Pemrosesan Informasi Federal \(FIPS\) 140-2](#).

Kami sangat merekomendasikan agar Anda tidak memasukkan informasi identifikasi sensitif apapun, seperti nomor rekening pelanggan Anda, ke dalam kolom isian teks bebas seperti kolom Nama. Ini termasuk saat Anda bekerja dengan Amazon Nimble Studio atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke Amazon Nimble Studio atau layanan lain mungkin diambil untuk dimasukkan dalam log diagnostik. Saat Anda memberikan URL ke server eksternal, jangan sertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

## Izin

Kelola akses ke AWS sumber daya menggunakan pengguna, peran IAM, dan dengan memberikan privasi paling sedikit kepada pengguna. Menetapkan kebijakan dan prosedur manajemen kredensial untuk membuat, mendistribusikan, memutar, dan mencabut kredensial AWS akses. Untuk informasi selengkapnya, lihat [Praktik Terbaik IAM](#) di Panduan Pengguna IAM.

# Support untuk Nimble ble ble ble ble ble ble ble ble ble ble

Bagian ini menyediakan opsi dukungan untuk Nimble Studio, seperti cara mendapatkan bantuan saat menerapkan atau menggunakan layanan dan aplikasi terkait.

## Daftar Isi

- [Nimble ble ble ble ble ble ble ble ble ble ble](#)
- [Dukungan aplikasi](#)
- [AWS SupportPusat](#)
- [AWS Supportrencana](#)

## Nimble ble ble ble ble ble ble ble ble ble ble

Jika Anda memiliki pertanyaan tentang Nimble Studio, Anda dapat mengunjungi forum [Nimble Studio](#). Di sana Anda bisa mendapatkan jawaban dari moderator komunitas dan AWS forum tentang fitur Nimble Studio, masalah teknis, dan bantuan pemecahan masalah.

## Dukungan aplikasi

Nimble Studio menyediakan dokumentasi tambahan untuk aplikasi berikut.

### AWSThinkboxDeadline

Untuk bantuan dengan pertanian render Anda atau untuk mempelajari cara Deadline kerjanya, lihat [AWSThinkboxDeadlinedokumentasi](#).

### Nimble ble ble ble ble ble ble ble ble File Transfer

Untuk mempelajari cara kerja Transfer File, lihat [Panduan Pengguna Transfer File Studio Nimble](#).

## AWS SupportPusat

[AWS SupportCenter](#) — Hub untuk membuat dan mengelola kasus dukungan Anda. Ini menyediakan akses ke berbagai sumber daya, termasuk solusi penagihan dan teknis, pusat pengetahuan, video pusat pengetahuan, AWS dokumentasi, ditambah pelatihan dan sertifikasi.

# AWS Supportrencana

AWS Supportpaket membantu Anda mengoptimalkan kinerja, tetap aman, menghindari waktu henti, dan mengendalikan biaya. Untuk informasi selengkapnya tentang AWS Support paket, lihat [Bandingkan AWS Support Paket](#).

Untuk informasi lebih lanjut tentang cara mendukung AWS Anda, kunjungi halaman [Hubungi kami](#).

## Riwayat dokumen

- Versi API: terbaru
- Pembaruan dokumentasi terbaru: 22 September 2023

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan Administrator Studio Nimble.

Perubahan	Deskripsi	
Layanan dan panduan baru	Ini adalah rilis awal Amazon Nimble Studio dan Panduan Administrator Amazon Nimble Studio.	Juni 19, 2023
AWS pembaruan kebijakan terkelola	Memperbarui AmazonNimbleStudio-StudioUser dan AmazonNimbleStudio-StudioAdmin kebijakan untuk menggunakan versi terbaru AWS IAM Identity Center layanan.	September 22, 2023

# AWSGlosarium

Untuk AWS terminologi terbaru, lihat [AWSglosarium di Referensi](#). Glosarium AWS



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