



Panduan Pengguna

Konsol Alat Developer



Konsol Alat Developer: Panduan Pengguna

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

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

Table of Contents

Apa yang dimaksud dengan konsol Alat Developer?	1
Apakah Anda pengguna baru?	3
Fitur konsol alat developer	3
Apa itu notifikasi?	4
Apa yang dapat saya lakukan dengan notifikasi?	4
Bagaimana notifikasi bekerja?	4
Bagaimana saya memulai dengan notifikasi?	4
Konsep notifikasi	5
Pengaturan	13
Memulai dengan notifikasi	20
Bekerja dengan aturan notifikasi	27
Bekerja dengan target aturan notifikasi	40
Konfigurasi integrasi antara notifikasi dan AWS Chatbot	49
Panggilan API AWS CodeStar Pemberitahuan Pencatatan dengan AWS CloudTrail	54
Pemecahan Masalah	58
Kuota	61
Apa itu koneksi?	61
Apa yang bisa saya lakukan dengan koneksi?	61
Untuk penyedia pihak ketiga apa saya dapat membuat koneksi?	62
Apa yang Layanan AWS terintegrasi dengan koneksi?	63
Bagaimana koneksi bekerja?	63
Sumber daya global di AWS CodeConnections	70
Bagaimana saya memulai dengan koneksi?	70
Konsep koneksi	71
AWS CodeConnections penyedia dan versi yang didukung	72
Integrasi produk dan layanan dengan AWS CodeConnections	73
Menyiapkan koneksi	76
Memulai dengan koneksi	78
Bekerja dengan koneksi	84
Bekerja dengan host	148
Bekerja dengan konfigurasi sinkronisasi untuk repositori tertaut	159
Logging koneksi panggilan API dengan CloudTrail	169
Titik akhir VPC (AWS PrivateLink)	210
Pemecahan masalah koneksi	213

Kuota	227
Alamat IP untuk ditambahkan ke daftar izin Anda	228
Keamanan	230
Memahami konten dan keamanan notifikasi	231
Perlindungan data	232
Manajemen identitas dan akses	233
Audiens	234
Mengautentikasi dengan identitas	234
Mengelola akses menggunakan kebijakan	235
Bagaimana fitur di konsol alat developer bekerja dengan IAM	236
AWS CodeConnections referensi izin	242
Contoh kebijakan berbasis identitas	258
Menggunakan tag untuk mengontrol akses ke AWS CodeConnections sumber daya	271
Menggunakan konsol	273
Izinkan para pengguna untuk melihat izin mereka sendiri	275
Pemecahan masalah	276
Menggunakan peran terkait layanan untuk Pemberitahuan AWS CodeStar	278
Menggunakan peran terkait layanan untuk AWS CodeConnections	283
AWS kebijakan terkelola	285
Validasi kepatuhan	288
Ketahanan	289
Keamanan infrastruktur	290
Lalu lintas antar AWS CodeConnections sumber daya lintas Wilayah	290
Ganti nama koneksi - Ringkasan perubahan	291
Awalan layanan berganti nama	291
Tindakan berganti nama di IAM	292
Sumber daya baru ARN	292
Kebijakan peran layanan yang terpengaruh	4
CloudFormation Sumber daya baru	4
Riwayat dokumen	293
AWS Glosarium	302
.....	ccciiii

Apa yang dimaksud dengan konsol Alat Developer?

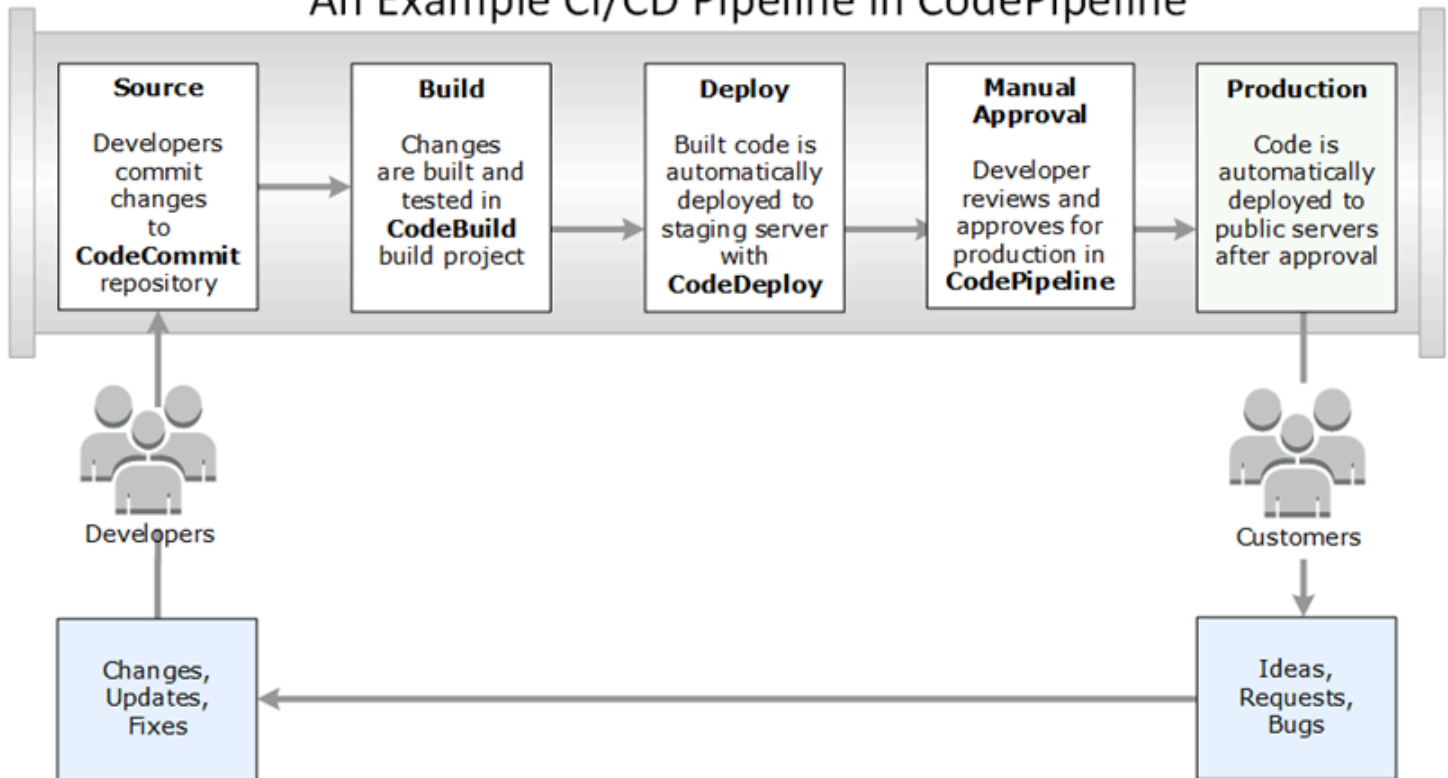
Konsol Alat Developer adalah rumah bagi serangkaian layanan dan fitur yang dapat Anda gunakan secara individual atau kolektif untuk membantu Anda mengembangkan perangkat lunak, baik secara individu maupun tim. Alat developer dapat membantu Anda menyimpan, membangun, menguji, dan men-deploy perangkat lunak Anda dengan aman. Digunakan secara individu atau kolektif, alat ini memberikan dukungan untuk DevOps, integrasi berkelanjutan, dan pengiriman berkelanjutan (CI/CD).

Konsol Alat Developer mencakup layanan berikut:

- [AWS CodeCommit](#) adalah layanan kontrol sumber terkelola penuh yang menghost repositori Git privat. Anda dapat menggunakan repositori untuk menyimpan dan mengelola aset secara pribadi (seperti dokumen, kode sumber, dan file biner) di file. AWS Cloud Repositori Anda menyimpan riwayat proyek Anda dari komit pertama hingga perubahan terbaru. Anda dapat bekerja secara kolaboratif pada kode di repositori dengan mengomentari kode dan membuat permintaan tarik untuk membantu memastikan kualitas kode.
- [AWS CodeBuild](#) adalah layanan build yang terkelola penuh yang mengompilasi kode sumber Anda, menjalankan tes unit, dan menghasilkan artefak yang siap dideploy. Ini menyediakan lingkungan bangunan yang dikemas untuk bahasa pemrograman populer dan membangun alat seperti Apache Maven, Gradle, dan banyak lagi. Anda juga dapat menyesuaikan lingkungan build CodeBuild untuk menggunakan alat build Anda sendiri.
- [AWS CodeDeploy](#) adalah layanan penyebaran terkelola penuh yang mengotomatiskan penerapan perangkat lunak untuk menghitung layanan seperti Amazon EC2 AWS Lambda, dan server lokal Anda. Hal ini dapat membantu Anda dengan cepat merilis fitur baru, menghindari downtime selama deployment aplikasi, dan menangani kompleksitas pembaruan aplikasi Anda.
- [AWS CodePipeline](#) adalah integrasi berkelanjutan dan layanan pengiriman berkelanjutan yang dapat Anda gunakan untuk memodelkan, memvisualisasikan, dan mengotomatiskan langkah-langkah yang diperlukan untuk merilis perangkat lunak Anda. Anda dapat dengan cepat memodelkan dan mengonfigurasi berbagai tahap proses rilis perangkat lunak. Anda dapat membangun, menguji, dan men-deploy kode Anda setiap kali ada perubahan kode, berdasarkan pada model proses rilis yang Anda definisikan.

Berikut adalah contoh bagaimana Anda dapat menggunakan layanan di konsol Alat Developer bersama-sama untuk membantu Anda mengembangkan perangkat lunak.

An Example CI/CD Pipeline in CodePipeline



Dalam contoh ini, pengembang membuat repositori CodeCommit dan menggunakannya untuk mengembangkan dan berkolaborasi pada kode mereka. Mereka membuat proyek build CodeBuild untuk membangun dan menguji kode mereka, dan menggunakannya CodeDeploy untuk menyebarkan kode mereka untuk menguji dan lingkungan produksi. Mereka ingin mengulangi dengan cepat, sehingga mereka membuat pipeline CodePipeline untuk mendeteksi perubahan dalam CodeCommit repositori. Perubahan-perubahan tersebut dibangun, tes dijalankan, dan kode yang berhasil dibangun dan diuji dikerahkan ke server pengujian. Tim menambahkan tahap uji alur untuk menjalankan tes lebih pada server tahap, seperti integrasi atau tes beban. Setelah berhasil menyelesaikan tes tersebut, seorang anggota tim meninjau hasilnya dan jika puas, secara manual menyetujui perubahan untuk produksi. CodePipeline menyebarkan kode yang diuji dan disetujui ke instance produksi.

Ini hanyalah salah satu contoh sederhana bagaimana Anda dapat menggunakan satu atau lebih layanan yang tersedia di konsol Alat Developer untuk membantu Anda mengembangkan perangkat lunak. Setiap layanan dapat disesuaikan sesuai kebutuhan Anda. Mereka menawarkan banyak integrasi dengan produk dan layanan lain, baik di dalam AWS maupun dengan alat pihak ketiga lainnya. Untuk informasi selengkapnya, lihat topik berikut:

- CodeCommit: [Integrasi produk dan layanan](#)

- CodeBuild: [Gunakan CodeBuild dengan Jenkins](#)
- CodeDeploy: [Integrasi produk dan layanan](#)
- CodePipeline: [Integrasi produk dan layanan](#)

Apakah Anda pengguna baru?

Jika Anda pengguna baru dari satu atau lebih layanan yang tersedia di konsol Alat Developer, sebaiknya mulai dengan membaca topik berikut:

- [Memulai dengan CodeCommit](#)
- [Memulai dengan CodeBuild, Konsep](#)
- [Memulai dengan CodeDeploy, Komponen utama](#)
- [Memulai dengan CodePipeline, Konsep](#)

Fitur konsol alat developer

Konsol Alat Developer mencakup fitur berikut:

- Konsol Alat Pengembang menyertakan fitur pengelola notifikasi yang dapat Anda gunakan untuk berlangganan acara di AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy, dan AWS CodePipeline. Fitur ini memiliki API sendiri, AWS CodeStar Notifikasi. Anda dapat menggunakan fitur notifikasi untuk segera memberitahu pengguna tentang peristiwa di repositori, membangun proyek, aplikasi deployment, dan alur yang paling penting untuk pekerjaan mereka. Manajer notifikasi membantu membuat pengguna menyadari peristiwa yang terjadi pada repositori, membangun, deployment, atau alur sehingga mereka dapat dengan cepat mengambil tindakan, seperti menyetujui perubahan atau mengoreksi kesalahan. Untuk informasi selengkapnya, lihat [Apa itu notifikasi?](#)
- Konsol Alat Pengembang menyertakan fitur koneksi yang dapat Anda gunakan untuk mengaitkan AWS sumber daya Anda dengan penyedia kode sumber pihak ketiga. Fitur ini memiliki API sendiri, AWS CodeConnections. Anda dapat menggunakan fitur koneksi untuk mengatur koneksi resmi dengan penyedia pihak ketiga dan menggunakan sumber daya koneksi dengan AWS layanan lain. Untuk informasi selengkapnya, lihat [Apa itu koneksi?](#)

Apa itu notifikasi?

Fitur notifikasi di konsol Alat Pengembang adalah pengelola notifikasi untuk berlangganan acara di AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy dan AWS CodePipeline. Ini memiliki API sendiri, AWS CodeStar Pemberitahuan. Anda dapat menggunakan fitur notifikasi untuk segera memberitahu pengguna tentang peristiwa di repositori, membangun proyek, aplikasi deployment, dan alur yang paling penting untuk pekerjaan mereka. Manajer notifikasi membantu membuat pengguna menyadari peristiwa yang terjadi pada repositori, membangun, deployment, atau alur sehingga mereka dapat dengan cepat mengambil tindakan, seperti menyetujui perubahan atau mengoreksi kesalahan.

Apa yang dapat saya lakukan dengan notifikasi?

Anda dapat menggunakan fitur notifikasi untuk membuat dan mengelola aturan notifikasi untuk memberi tahu pengguna tentang perubahan penting pada sumber daya mereka, termasuk:

- Membangun keberhasilan dan kegagalan dalam CodeBuild membangun proyek.
- Keberhasilan dan kegagalan penerapan dalam CodeDeploy aplikasi.
- Pembuatan dan pembaruan dalam permintaan tarik, termasuk komentar pada kode, di CodeCommit repositori.
- Status persetujuan manual dan pipeline berjalan di CodePipeline.

Anda dapat mengatur notifikasi sehingga bisa menuju ke alamat email pengguna yang berlangganan topik Amazon SNS. Anda juga dapat mengintegrasikan fitur ini dengan [AWS Chatbot](#) dan mengirimkan notifikasi ke saluran Slack, saluran Microsoft Teams, atau ruang obrolan Amazon Chime.

Bagaimana notifikasi bekerja?

Saat Anda mengonfigurasi aturan notifikasi untuk sumber daya yang didukung, seperti repositori, proyek build, aplikasi, atau pipeline, fitur notifikasi akan membuat EventBridge aturan Amazon yang memantau peristiwa yang Anda tentukan. Ketika peristiwa dari jenis tersebut terjadi, aturan notifikasi mengirimkan notifikasi ke topik Amazon SNS ditetapkan sebagai target untuk aturan itu. Pelanggan target tersebut menerima notifikasi tentang peristiwa tersebut.

Bagaimana saya memulai dengan notifikasi?

Untuk memulai, berikut adalah beberapa topik yang berguna untuk ditinjau:

- Pelajari tentang [konsep](#) untuk notifikasi.
- Menyiapkan [sumber daya yang Anda butuhkan](#) untuk mulai bekerja dengan notifikasi.
- Memulai dengan [aturan notifikasi pertama](#) dan menerima notifikasi pertama Anda.

Konsep notifikasi

Menyiapkan dan menggunakan notifikasi lebih mudah jika Anda memahami konsep dan istilahnya. Berikut adalah beberapa konsep yang perlu diketahui saat Anda menggunakan notifikasi.

Topik

- [Notifikasi](#)
- [Aturan notifikasi](#)
- [Peristiwa](#)
- [Jenis detail](#)
- [Target](#)
- [Pemberitahuan dan AWS CodeStar Pemberitahuan](#)
- [Peristiwa untuk aturan notifikasi pada repositori](#)
- [Acara untuk aturan notifikasi tentang proyek build](#)
- [Peristiwa untuk aturan notifikasi pada aplikasi deployment](#)
- [Acara untuk aturan notifikasi pada alur](#)

Notifikasi

Sebuah notifikasi adalah pesan yang berisi informasi tentang peristiwa yang terjadi di sumber daya yang Anda dan developer Anda gunakan. Anda dapat mengatur notifikasi sehingga pengguna sumber daya, seperti membangun proyek, repositori, aplikasi deployment, atau alur, menerima email tentang jenis acara yang Anda tentukan sesuai dengan aturan notifikasi yang Anda buat.

Pemberitahuan untuk AWS CodeCommit dapat berisi informasi identitas pengguna, seperti nama tampilan atau alamat email, melalui penggunaan tag sesi. CodeCommit mendukung penggunaan tag sesi, yang merupakan atribut pasangan nilai kunci yang Anda lewati saat Anda mengambil peran IAM, menggunakan kredensi sementara, atau menyatukan pengguna di (). AWS Security Token Service AWS STS Anda juga dapat mengaitkan tag dengan pengguna IAM. CodeCommit termasuk

nilai untuk `displayName` dan `emailAddress` dalam konten notifikasi jika tag tersebut ada. Untuk informasi selengkapnya, lihat [Menggunakan tag untuk memberikan informasi identitas tambahan di CodeCommit](#).

Important

Notifikasi mencakup informasi spesifik proyek seperti status build, status deployment, baris kode yang memiliki komentar, dan persetujuan alur. Konten notifikasi dapat berubah saat fitur baru ditambahkan. Sebagai praktik terbaik keamanan, Anda harus secara teratur meninjau target aturan notifikasi dan pelanggan topik Amazon SNS. Untuk informasi lebih lanjut, lihat [Memahami konten dan keamanan notifikasi](#).

Aturan notifikasi

Aturan notifikasi adalah AWS sumber daya yang Anda buat untuk menentukan kapan dan di mana notifikasi dikirim. Ini mendefinisikan:

- Kondisi di mana notifikasi dibuat. Kondisi ini didasarkan pada peristiwa yang Anda pilih, yang spesifik untuk jenis sumber daya. Jenis sumber daya yang didukung termasuk proyek pembangunan AWS CodeBuild, aplikasi penerapan di AWS CodeDeploy, saluran pipa AWS CodePipeline, dan repositori di AWS CodeCommit
- Target yang dikirim notifikasi. Anda dapat menentukan hingga 10 target untuk aturan notifikasi.

Aturan notifikasi dicakup untuk proyek build individu, aplikasi deployment, alur, dan repositori. Aturan notifikasi memiliki nama ramah yang ditentukan pengguna dan Nama Sumber Daya Amazon (ARNs). Aturan pemberitahuan harus dibuat di AWS Wilayah yang sama di mana sumber daya ada. Misalnya, jika proyek build Anda berada di Wilayah US East (Ohio), aturan notifikasi Anda harus dibuat di Wilayah US East (Ohio) juga.

Anda dapat menentukan hingga 10 aturan notifikasi untuk sumber daya.

Peristiwa

Sebuah peristiwa adalah perubahan status pada sumber daya yang ingin Anda pantau. Setiap sumber daya memiliki daftar jenis acara yang dapat Anda pilih. Ketika Anda mengatur aturan notifikasi pada sumber daya, Anda menentukan peristiwa yang menyebabkan notifikasi dikirim. Misalnya, jika Anda mengatur notifikasi untuk repositori di CodeCommit, dan Anda memilih Dibuat

untuk permintaan Tarik dan Cabang dan tag, pemberitahuan akan dikirim setiap kali pengguna di repositori tersebut membuat permintaan tarik, cabang, atau tag Git.

Jenis detail

Saat membuat aturan notifikasi, Anda dapat memilih tingkat detail atau tipe detail termasuk dalam notifikasi (Penuh atau Basic). Pengaturan Penuh (default) mencakup semua informasi yang tersedia untuk acara dalam notifikasi, termasuk informasi yang disempurnakan yang disediakan oleh layanan untuk acara tertentu. Pengaturan Basic mencakup hanya subset dari informasi yang tersedia.

Tabel berikut mencantumkan informasi yang disempurnakan yang tersedia untuk jenis acara tertentu dan menjelaskan perbedaan antara jenis detail.

Layanan	Peristiwa	Full termasuk	Basic tidak termasuk
CodeCommit	Komentar pada komit Komentar pada permintaan tarik	Semua detail acara dan isi komentar, termasuk balasan atau utas komentar. Ini juga mencakup nomor baris dan baris kode di mana komentar dibuat.	Isi komentar. nomor baris, baris kode, atau utas komentar apa pun.
CodeCommit	Permintaan tarik dibuat	Semua detail peristiwa dan jumlah file yang ditambahkan, dimodifikasi, atau dihapus dalam permintaan tarik dalam kaitannya dengan cabang tujuan.	Tidak ada daftar file atau detail tentang apakah cabang sumber permintaan tarik telah menambahkan, mengubah, atau menghapus file.
CodePipeline	Persetujuan manual diperlukan	Semua detail acara dan data kustom (jika dikonfigurasi). Notifikasi ini juga	Tidak ada data atau tautan kustom.

Layanan	Peristiwa	Full termasuk	Basic tidak termasuk
		mencakup tautan ke persetujuan yang diperlukan dalam alur.	
CodePipeline	Eksekusi tindakan gagal Eksekusi alur gagal Eksekusi tahap gagal	Semua detail acara dan isi dari pesan kesalahan untuk kegagalan.	Tidak ada isi pesan kesalahan.

Target

Sebuah target adalah lokasi untuk menerima notifikasi dari aturan notifikasi. Jenis target yang diizinkan adalah topik Amazon SNS dan klien Chatbot yang dikonfigurasi untuk AWS saluran Slack atau Microsoft Teams. Setiap pengguna yang berlangganan target menerima notifikasi tentang peristiwa yang Anda tentukan dalam aturan notifikasi.

Jika Anda ingin memperluas jangkauan notifikasi, Anda dapat mengonfigurasi integrasi antara notifikasi dan AWS Chatbot secara manual sehingga notifikasi dikirim ke ruang obrolan Amazon Chime. Anda kemudian dapat memilih topik Amazon SNS yang dikonfigurasi untuk klien Chatbot AWS tersebut sebagai target untuk aturan notifikasi. Untuk informasi selengkapnya, lihat [Untuk mengintegrasikan notifikasi dengan AWS Chatbot dan Amazon Chime](#).

Jika Anda memilih untuk menggunakan klien AWS Chatbot sebagai target, Anda harus terlebih dahulu membuat klien itu di AWS Chatbot. Saat Anda memilih klien AWS Chatbot sebagai target untuk aturan notifikasi, topik Amazon SNS dikonfigurasi untuk klien AWS Chatbot tersebut dengan semua kebijakan yang diperlukan agar notifikasi dikirim ke saluran Slack atau Microsoft Teams. Anda tidak perlu mengonfigurasi topik Amazon SNS yang ada untuk klien Chatbot AWS .

Anda dapat memilih untuk membuat topik Amazon SNS sebagai target sebagai bagian dari pembuatan aturan notifikasi (disarankan). Anda juga dapat memilih topik Amazon SNS yang ada di AWS Wilayah yang sama dengan aturan notifikasi, tetapi Anda harus mengonfigurasinya dengan kebijakan yang diperlukan. Topik Amazon SNS yang Anda gunakan untuk target harus ada di akun Anda AWS . Itu juga harus berada di AWS Wilayah yang sama dengan aturan notifikasi dan AWS sumber daya tempat aturan itu dibuat.

Misalnya, jika Anda membuat aturan notifikasi untuk repositori di Wilayah US East (Ohio), topik Amazon SNS juga harus ada di Wilayah tersebut. Jika Anda membuat topik Amazon SNS sebagai bagian dari membuat aturan notifikasi, topik dikonfigurasi dengan kebijakan yang diperlukan untuk memungkinkan publikasi peristiwa untuk topik. Ini adalah metode terbaik untuk bekerja dengan target dan aturan notifikasi. Jika Anda memilih untuk menggunakan topik yang sudah ada atau membuatnya secara manual, Anda harus mengonfigurasinya dengan izin yang diperlukan sebelum pengguna menerima notifikasi. Untuk informasi lebih lanjut, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#).

Note

Jika Anda ingin menggunakan topik Amazon SNS yang sudah ada alih-alih membuat yang baru, di Target, pilih ARN-nya. Pastikan topik memiliki kebijakan akses yang sesuai, dan daftar pelanggan hanya berisi pengguna yang diizinkan untuk melihat informasi tentang sumber daya. Jika topik Amazon SNS adalah topik yang digunakan untuk CodeCommit pemberitahuan sebelum 5 November 2019, itu akan berisi kebijakan yang memungkinkan CodeCommit untuk mempublikasikannya yang berisi izin berbeda dari yang diperlukan untuk Pemberitahuan. AWS CodeStar Menggunakan topik ini tidak disarankan. Jika Anda ingin menggunakan yang dibuat untuk pengalaman itu, Anda harus menambahkan kebijakan yang diperlukan untuk AWS CodeStar Pemberitahuan selain yang sudah ada. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) dan [Memahami konten dan keamanan notifikasi](#).

Pemberitahuan dan AWS CodeStar Pemberitahuan

Sementara fitur konsol Alat Pengembang, notifikasi memiliki API sendiri, AWS CodeStar Pemberitahuan. Ia juga mempunyai jenis sumber daya AWS sendiri (aturan notifikasi), izin, dan peristiwa. Peristiwa untuk aturan notifikasi masuk AWS CloudTrail. Tindakan API dapat diizinkan atau ditolak melalui kebijakan IAM.

Peristiwa untuk aturan notifikasi pada repositori

Kategori	Peristiwa	Acara IDs
Komentari	Pada komit	codecommit-repository-
	Pada permintaan tarik	comments-on-commits

Kategori	Peristiwa	Acara IDs
		<code>codecommit-repository-comments-on-pull-requests</code>
Persetujuan	Status berubah Menimpa aturan	<code>codecommit-repository-approvals-status-changed</code> <code>codecommit-repository-approvals-rule-override</code>
Permintaan tarik	Dibuat Sumber diperbarui Status berubah Digabungkan	<code>codecommit-repository-pull-request-created</code> <code>codecommit-repository-pull-request-source-updated</code> <code>codecommit-repository-pull-request-status-changed</code> <code>codecommit-repository-pull-request-merged</code>
Cabang dan tanda	Dibuat Dihapus Diperbarui	<code>codecommit-repository-branches-and-tags-created</code> <code>codecommit-repository-branches-and-tags-deleted</code> <code>codecommit-repository-branches-and-tags-updated</code>

Acara untuk aturan notifikasi tentang proyek build

Kategori	Peristiwa	Acara IDs
Status build	Gagal	codebuild-project-build-state-failed
	Berhasil	codebuild-project-build-state-succeeded
	Sedang berlangsung	codebuild-project-build-state-in-progress
	Dihentikan	codebuild-project-build-state-stopped
Tahap membangun	Kegagalan	codebuild-project-build-phase-failure
	Sukses	codebuild-project-build-phase-success

Peristiwa untuk aturan notifikasi pada aplikasi deployment

Kategori	Peristiwa	Acara IDs
Deployment	Gagal	codedeploy-application-deployment-failed
	Berhasil	codedeploy-application-deployment-succeeded
	Dimulai	codedeploy-application-deployment-started

Acara untuk aturan notifikasi pada alur

Kategori	Peristiwa	Acara IDs
Eksekusi tindakan	Berhasil	<code>codepipeline-pipeline-action-execution-succeeded</code>
	Gagal	
	Dibatalkan	<code>codepipeline-pipeline-action-execution-failed</code>
	Dimulai	<code>codepipeline-pipeline-action-execution-canceled</code>
		<code>codepipeline-pipeline-action-execution-started</code>
Eksekusi tahap	Dimulai	<code>codepipeline-pipeline-stage-execution-started</code>
	Berhasil	
	Dilanjutkan	<code>codepipeline-pipeline-stage-execution-succeeded</code>
	Dibatalkan	<code>codepipeline-pipeline-stage-execution-resumed</code>
	Gagal	<code>codepipeline-pipeline-stage-execution-canceled</code>
	<code>codepipeline-pipeline-stage-execution-failed</code>	
Eksekusi alur	Gagal	<code>codepipeline-pipeline-pipeline-execution-failed</code>
	Dibatalkan	
	Dimulai	<code>codepipeline-pipeline-pipeline-execution-canceled</code>
	Dilanjutkan	
	Berhasil	<code>codepipeline-pipeline-pipeline-execution-started</code>

Kategori	Peristiwa	Acara IDs
	Digantikan	codepipeline-pipeline-pipeline-execution-resumed codepipeline-pipeline-pipeline-execution-succeeded codepipeline-pipeline-pipeline-execution-superseded
Persetujuan manual	Gagal	codepipeline-pipeline-manual-approval-failed
	Diperlukan	codepipeline-pipeline-manual-approval-needed
	Berhasil	codepipeline-pipeline-manual-approval-succeeded

Pengaturan

Jika Anda memiliki kebijakan terkelola untuk AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy, atau AWS CodePipeline diterapkan pada pengguna atau peran IAM Anda, Anda memiliki izin yang diperlukan untuk bekerja dengan pemberitahuan dalam batasan peran dan izin yang disediakan oleh kebijakan. Sebagai contoh, pengguna yang memiliki kebijakan terkelola `AWSCodeBuildAdminAccess`, `AWSCodeCommitFullAccess`, `AWSCodeDeployFullAccess`, atau `AWSCodePipeline_FullAccess` yang diterapkan memiliki akses administratif penuh ke notifikasi.

Untuk informasi selengkapnya, termasuk kebijakan contoh, lihat [Kebijakan berbasis identitas](#).

Jika salah satu kebijakan ini diterapkan pada pengguna atau peran IAM Anda, dan proyek build di CodeBuild, repositori di CodeCommit, aplikasi penerapan, atau pipeline di CodeDeploy CodePipeline, Anda siap untuk membuat aturan notifikasi pertama Anda. Lanjutkan ke [Memulai dengan notifikasi](#). Jika tidak, lihat topik berikut:

- CodeBuild: [Memulai dengan CodeBuild](#)
- CodeCommit: [Memulai dengan CodeCommit](#)

- CodeDeploy: [Tutorial](#)
- CodePipeline: [Memulai dengan CodePipeline](#)

Jika Anda ingin mengelola izin administratif untuk notifikasi bagi pengguna IAM, grup, atau peran sendiri, ikuti prosedur dalam topik ini untuk mengatur izin dan sumber daya yang Anda butuhkan untuk menggunakan layanan.

Jika Anda ingin menggunakan topik Amazon SNS yang dibuat sebelumnya untuk notifikasi bukannya membuat topik khusus untuk notifikasi, Anda harus mengonfigurasi topik Amazon SNS untuk digunakan sebagai target untuk aturan notifikasi dengan menerapkan kebijakan yang memungkinkan peristiwa untuk diterbitkan untuk topik tersebut.

Note

Untuk melakukan prosedur berikut, Anda harus masuk dengan akun yang memiliki izin administratif. Untuk informasi selengkapnya, lihat [Membuat pengguna dan grup admin IAM pertama Anda](#).

Topik

- [Membuat dan menerapkan kebijakan untuk akses administratif ke notifikasi](#)
- [Mengonfigurasi topik Amazon SNS untuk notifikasi](#)
- [Berlangganan pengguna ke topik Amazon SNS yang menjadi target](#)

Membuat dan menerapkan kebijakan untuk akses administratif ke notifikasi

Anda dapat mengelola pemberitahuan dengan masuk dengan pengguna IAM atau menggunakan peran yang memiliki izin untuk mengakses layanan dan layanan (AWS CodeBuild,, AWS CodeCommit AWS CodeDeploy, atau AWS CodePipeline) yang ingin Anda buat notifikasi. Anda juga dapat membuat kebijakan Anda sendiri dan menerapkannya ke pengguna atau grup.

Prosedur berikut menunjukkan cara mengonfigurasi grup IAM dengan izin untuk mengelola notifikasi dan menambahkan pengguna IAM. Jika Anda tidak ingin membuat grup, Anda dapat menerapkan kebijakan ini secara langsung ke pengguna IAM atau IAM role yang dapat diasumsikan oleh pengguna. Anda juga dapat menggunakan kebijakan terkelola untuk CodeBuild, CodeCommit, CodeDeploy, atau CodePipeline, yang mencakup akses sesuai kebijakan ke fitur notifikasi tergantung pada ruang lingkup kebijakan.

Untuk kebijakan di bawah ini, masukkan nama (misalnya, `AWSCodeStarNotificationsFullAccess`) dan deskripsi opsional untuk kebijakan ini. Deskripsi membantu Anda mengingat tujuan kebijakan (misalnya, **This policy provides full access to AWS CodeStar Notifications.**)

Cara menggunakan editor kebijakan JSON untuk membuat kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Pada panel navigasi di sebelah kiri, pilih Kebijakan.

Jika ini pertama kalinya Anda memilih Kebijakan, akan muncul halaman Selamat Datang di Kebijakan Terkelola. Pilih Memulai.

3. Di bagian atas halaman, pilih Buat kebijakan.
4. Di bagian Editor kebijakan, pilih opsi JSON.
5. Masukkan dokumen kebijakan JSON berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCodeStarNotificationsFullAccess",
      "Effect": "Allow",
      "Action": [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications>DeleteNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe",
        "codestar-notifications>DeleteTarget",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsForResource",
        "codestar-notifications:TagResource",
        "codestar-notifications:UntagResource"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

6. Pilih Berikutnya.

Note

Anda dapat beralih antara opsi editor Visual dan JSON kapan saja. Namun, jika Anda melakukan perubahan atau memilih Berikutnya di editor Visual, IAM dapat merestrukturisasi kebijakan Anda untuk mengoptimalkannya bagi editor visual. Untuk informasi selengkapnya, lihat [Restrukturisasi kebijakan](#) dalam Panduan Pengguna IAM.

7. Pada halaman Tinjau dan buat, masukkan Nama kebijakan dan Deskripsi (opsional) untuk kebijakan yang Anda buat. Tinjau Izin yang ditentukan dalam kebijakan ini untuk melihat izin yang diberikan oleh kebijakan Anda.
8. Pilih Buat kebijakan untuk menyimpan kebijakan baru Anda.

Mengonfigurasi topik Amazon SNS untuk notifikasi

Cara termudah untuk mengatur notifikasi adalah untuk membuat topik Amazon SNS ketika Anda membuat aturan notifikasi. Anda dapat menggunakan topik Amazon SNS yang sudah ada jika memenuhi persyaratan berikut:

- Itu dibuat Wilayah AWS sama dengan sumber daya (proyek build, aplikasi penerapan, repositori, atau pipeline) yang ingin Anda buat aturan notifikasi.
- Ini belum digunakan untuk mengirim pemberitahuan CodeCommit sebelum 5 November 2019. Jika memiliki, itu akan berisi pernyataan kebijakan yang memungkinkan fungsionalitas tersebut. Anda dapat memilih untuk menggunakan topik ini, namun Anda perlu menambahkan kebijakan tambahan seperti yang ditentukan dalam prosedur. Anda tidak boleh menghapus pernyataan kebijakan yang ada jika satu atau beberapa repositori masih dikonfigurasi untuk notifikasi sebelum 5 November 2019.
- Ini memiliki kebijakan yang memungkinkan AWS CodeStar Pemberitahuan untuk mempublikasikan pemberitahuan ke topik.

Untuk mengonfigurasi topik Amazon SNS agar digunakan sebagai target aturan AWS CodeStar pemberitahuan Pemberitahuan

1. [Masuk ke Konsol Manajemen AWS dan buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Di bilah navigasi, pilih Topik, pilih topik yang ingin Anda konfigurasi, lalu pilih Edit.
3. Perluas Kebijakan akses, lalu pilih Lanjutkan.
4. Pada editor JSON, tambahkan pernyataan berikut ke kebijakan. Sertakan topik ARN,, Akun AWS ID Wilayah AWS, dan nama topik.

```
{
  "Sid": "AWSCodeStarNotifications_publish",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "codestar-notifications.amazonaws.com"
    ]
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-MyTopicForNotificationRules"
}
```

Pernyataan kebijakan akan terlihat seperti berikut.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "SNS:AddPermission",
        "SNS:RemovePermission",
        "SNS>DeleteTopic",

```

```

    "SNS:Subscribe",
    "SNS:ListSubscriptionsByTopic",
    "SNS:Publish"
  ],
  "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-MyTopicForNotificationRules",
  "Condition": {
    "StringEquals": {
      "AWS:SourceOwner": "123456789012"
    }
  }
},
{
  "Sid": "AWSCodeStarNotifications_publish",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "codestar-notifications.amazonaws.com"
    ]
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-MyTopicForNotificationRules"
}
]
}

```

5. Pilih Simpan perubahan.
6. Jika Anda ingin menggunakan topik Amazon AWS KMS SNS yang dienkripsi untuk mengirim notifikasi, Anda juga harus mengaktifkan kompatibilitas antara sumber peristiwa (AWS CodeStar Pemberitahuan) dan topik terenkripsi dengan menambahkan pernyataan berikut ke kebijakan. AWS KMS key Ganti Wilayah AWS (dalam contoh ini, us-east-2) dengan Wilayah AWS tempat kunci dibuat.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {

```

```
        "Service": "codestar-notifications.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "sns.us-east-2.amazonaws.com"
        }
    }
}
]
```

Untuk informasi selengkapnya, lihat [Enkripsi saat diam](#) dan [Menggunakan syarat kebijakan dengan AWS KMS](#) di AWS Key Management Service Panduan Developer.

Berlangganan pengguna ke topik Amazon SNS yang menjadi target

Sebelum pengguna dapat menerima notifikasi, mereka harus berlangganan topik Amazon SNS yang merupakan target aturan notifikasi. Jika pengguna berlangganan melalui alamat email, mereka harus mengonfirmasi langganan mereka sebelum menerima notifikasi. Untuk mengirim notifikasi ke pengguna di saluran Slack, saluran Microsoft Teams, atau ruang obrolan Amazon Chime, lihat [Konfigurasi integrasi antara notifikasi dan AWS Chatbot](#)

Untuk berlangganan pengguna ke topik Amazon SNS yang digunakan untuk notifikasi

1. [Masuk ke Konsol Manajemen AWS dan buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Di bilah navigasi, pilih Topik, dan kemudian pilih topik yang Anda ingin berlangganan pengguna.
3. Di Langganan, pilih Buat langganan.
4. Di Protokol, pilih Email. Di Titik akhir, masukkan alamat email, lalu pilih Buat langganan.

Memulai dengan notifikasi

Cara termudah untuk memulai notifikasi adalah dengan menyiapkan aturan notifikasi di salah satu proyek build, aplikasi deployment, alur, atau repositori Anda.

Note

Saat pertama kali Anda membuat aturan notifikasi, sebuah peran terkait layanan dibuat di akun Anda. Untuk informasi lebih lanjut, lihat [Menggunakan peran terkait layanan untuk Pemberitahuan AWS CodeStar](#).

Topik

- [Prasyarat](#)
- [Membuat aturan notifikasi untuk repositori](#)
- [Buat aturan notifikasi untuk membangun proyek](#)
- [Membuat aturan notifikasi untuk aplikasi deployment](#)
- [Membuat aturan notifikasi untuk alur](#)

Prasyarat

Selesaikan langkah-langkah dalam [Pengaturan](#). Anda juga memerlukan sumber daya yang Anda buatkan aturan notifikasinya.

- [Buat proyek build CodeBuild](#) atau gunakan yang sudah ada.
- [Buat aplikasi](#) atau gunakan aplikasi deployment yang sudah ada.
- [Buat pipeline CodePipeline](#) atau gunakan yang sudah ada.
- [Buat AWS CodeCommit repositori](#) atau gunakan yang sudah ada.

Membuat aturan notifikasi untuk repositori

Anda dapat membuat aturan notifikasi untuk mengirim notifikasi tentang peristiwa repositori yang penting bagi Anda. Langkah-langkah berikut menunjukkan cara mengatur aturan notifikasi pada acara repositori tunggal. Langkah-langkah ini ditulis dengan asumsi bahwa Anda memiliki repositori yang dikonfigurasi di akun Anda. AWS

Important

Jika Anda mengatur notifikasi CodeCommit sebelum 5 November 2019, topik Amazon SNS yang digunakan untuk notifikasi tersebut akan berisi kebijakan yang memungkinkan CodeCommit untuk mempublikasikannya yang berisi izin berbeda dari yang diperlukan untuk Pemberitahuan. AWS CodeStar Menggunakan topik ini tidak disarankan. Jika Anda ingin menggunakan yang dibuat untuk pengalaman itu, Anda harus menambahkan kebijakan yang diperlukan untuk AWS CodeStar Pemberitahuan selain yang sudah ada. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) dan [Memahami konten dan keamanan notifikasi](#).

1. Buka CodeCommit konsol di <https://console.aws.amazon.com/codecommit/>.
2. Pilih repositori dari daftar dan buka.
3. Pilih Beri tahu, lalu pilih Buat aturan notifikasi. Anda juga dapat memilih Pengaturan, pilihNotifikasi, lalu pilih Buat aturan notifikasi.
4. Di Nama notifikasi, masukkan nama untuk aturan.
5. Di Jenis detail, pilih Dasar jika Anda hanya menginginkan informasi yang diberikan ke Amazon yang EventBridge disertakan dalam notifikasi. Pilih Lengkap jika Anda ingin menyertakan informasi yang diberikan ke Amazon EventBridge dan informasi yang mungkin disediakan oleh layanan sumber daya atau pengelola notifikasi.

Untuk informasi selengkapnya, lihat [Memahami konten dan keamanan notifikasi](#).

6. Di Peristiwa yang memicu notifikasi, di bawah Cabang dan tanda pilih, pilih Dibuat.
7. Di Target, pilih Buat topik SNS.

Note

Saat Anda membuat topik sebagai bagian dari pembuatan aturan notifikasi, kebijakan yang memungkinkan CodeCommit untuk mempublikasikan peristiwa ke topik diterapkan untuk Anda. Menggunakan topik yang dibuat untuk aturan notifikasi membantu memastikan bahwa Anda hanya berlangganan pengguna yang ingin Anda terima notifikasi tentang repositori ini.

Setelah prefiks `codestar-notifications-`, masukkan nama untuk topik, lalu pilih nama, lalu pilih Kirim.

Note

Jika Anda ingin menggunakan topik Amazon SNS yang sudah ada alih-alih membuat yang baru, di Target, pilih ARN-nya. Pastikan topik memiliki kebijakan akses yang sesuai, dan daftar pelanggan hanya berisi pengguna yang diizinkan untuk melihat informasi tentang sumber daya. Jika topik Amazon SNS adalah topik yang digunakan untuk CodeCommit pemberitahuan sebelum 5 November 2019, itu akan berisi kebijakan yang memungkinkan CodeCommit untuk mempublikasikannya yang berisi izin berbeda dari yang diperlukan untuk Pemberitahuan. AWS CodeStar Menggunakan topik ini tidak disarankan. Jika Anda ingin menggunakan yang dibuat untuk pengalaman itu, Anda harus menambahkan kebijakan yang diperlukan untuk AWS CodeStar Pemberitahuan selain yang sudah ada. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) dan [Memahami konten dan keamanan notifikasi](#).

8. Pilih Kirim, dan kemudian tinjau aturan notifikasi.
9. Berlangganan alamat email Anda ke topik Amazon SNS yang baru saja Anda buat. Untuk informasi lebih lanjut, lihat [Untuk berlangganan pengguna ke topik Amazon SNS yang digunakan untuk notifikasi](#).
10. Arahkan ke repositori Anda dan buat cabang uji dari cabang default.
11. Setelah Anda membuat cabang, aturan notifikasi mengirimkan notifikasi ke semua pelanggan topik dengan informasi tentang acara tersebut.

Buat aturan notifikasi untuk membangun proyek

Anda dapat membuat aturan notifikasi untuk mengirim notifikasi tentang peristiwa pada proyek build yang penting bagi Anda. Langkah-langkah berikut menunjukkan cara mengatur aturan notifikasi pada acara proyek build tunggal. Langkah-langkah ini ditulis dengan asumsi bahwa Anda memiliki proyek build yang dikonfigurasi di AWS akun Anda.

1. Buka CodeBuild konsol di <https://console.aws.amazon.com/codebuild/>.
2. Pilih proyek build dari daftar dan buka.

3. Pilih Beri tahu, lalu pilih Buat aturan notifikasi. Anda juga dapat memilih Pengaturan, lalu pilih Buat aturan notifikasi.
4. Di Nama notifikasi, masukkan nama untuk aturan.
5. Di Jenis detail, pilih Dasar jika Anda hanya menginginkan informasi yang diberikan ke Amazon yang EventBridge disertakan dalam notifikasi. Pilih Lengkap jika Anda ingin menyertakan informasi yang diberikan ke Amazon EventBridge dan informasi yang mungkin disediakan oleh layanan sumber daya atau pengelola notifikasi.

Untuk informasi selengkapnya, lihat [Memahami konten dan keamanan notifikasi](#).

6. Di Peristiwa yang memicu notifikasi, di bawah Tahap pembuatan, pilih Sukses.
7. Di Target, pilih Buat topik SNS.

Note

Saat Anda membuat topik sebagai bagian dari pembuatan aturan notifikasi, kebijakan yang memungkinkan CodeBuild untuk mempublikasikan peristiwa ke topik diterapkan untuk Anda. Menggunakan topik yang dibuat untuk aturan notifikasi membantu memastikan bahwa Anda hanya berlangganan pengguna yang ingin Anda terima notifikasi tentang proyek build ini.

Setelah prefiks `codestar-notifications-`, masukkan nama untuk topik, lalu pilih Kirim.

Note

Jika Anda ingin menggunakan topik Amazon SNS yang sudah ada alih-alih membuat yang baru, di Target, pilih ARN-nya. Pastikan topik memiliki kebijakan akses yang sesuai, dan daftar pelanggan hanya berisi pengguna yang diizinkan untuk melihat informasi tentang sumber daya. Jika topik Amazon SNS adalah topik yang digunakan untuk CodeCommit pemberitahuan sebelum 5 November 2019, itu akan berisi kebijakan yang memungkinkan CodeCommit untuk mempublikasikannya yang berisi izin berbeda dari yang diperlukan untuk Pemberitahuan. AWS CodeStar Menggunakan topik ini tidak disarankan. Jika Anda ingin menggunakan yang dibuat untuk pengalaman itu, Anda harus menambahkan kebijakan yang diperlukan untuk AWS CodeStar Pemberitahuan

selain yang sudah ada. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) dan [Memahami konten dan keamanan notifikasi](#).

8. Pilih Kirim, dan kemudian tinjau aturan notifikasi.
9. Berlangganan alamat email Anda ke topik Amazon SNS yang baru saja Anda buat. Untuk informasi lebih lanjut, lihat [Untuk berlangganan pengguna ke topik Amazon SNS yang digunakan untuk notifikasi](#).
10. Arahkan ke proyek build Anda dan mulai membangun.
11. Setelah tahap membangun berhasil diselesaikan, aturan notifikasi mengirimkan notifikasi ke semua pelanggan topik dengan informasi tentang acara tersebut.

Membuat aturan notifikasi untuk aplikasi deployment

Anda dapat membuat aturan notifikasi untuk mengirim notifikasi tentang peristiwa pada aplikasi deployment Anda yang penting bagi Anda. Langkah-langkah berikut menunjukkan cara mengatur aturan notifikasi pada acara proyek build tunggal. Langkah-langkah ini ditulis dengan asumsi bahwa Anda memiliki aplikasi deployment yang dikonfigurasi di akun AWS .

1. Buka CodeDeploy konsol di <https://console.aws.amazon.com/codedeploy/>.
2. Pilih aplikasi dari daftar dan buka.
3. Pilih Beri tahu, lalu pilih Buat aturan notifikasi. Anda juga dapat memilih Pengaturan, lalu pilih Buat aturan notifikasi.
4. Di Nama notifikasi, masukkan nama untuk aturan.
5. Di Jenis detail, pilih Dasar jika Anda hanya menginginkan informasi yang diberikan ke Amazon yang EventBridge disertakan dalam notifikasi. Pilih Lengkap jika Anda ingin menyertakan informasi yang diberikan ke Amazon EventBridge dan informasi yang mungkin disediakan oleh layanan sumber daya atau pengelola notifikasi.

Untuk informasi selengkapnya, lihat [Memahami konten dan keamanan notifikasi](#).

6. Di Peristiwa yang memicu notifikasi, di bawah Deployment, pilih Berhasil.
7. Di Target, pilih Buat topik SNS.

Note

Saat Anda membuat topik sebagai bagian dari pembuatan aturan notifikasi, kebijakan yang memungkinkan CodeDeploy untuk mempublikasikan peristiwa ke topik diterapkan untuk Anda. Menggunakan topik yang dibuat untuk aturan notifikasi membantu memastikan bahwa Anda hanya berlangganan pengguna yang ingin Anda terima notifikasi tentang aplikasi deployment ini.

Setelah prefiks `codestar-notifications-`, masukkan nama untuk topik, lalu pilih Kirim.

Note

Jika Anda ingin menggunakan topik Amazon SNS yang sudah ada alih-alih membuat yang baru, di Target, pilih ARN-nya. Pastikan topik memiliki kebijakan akses yang sesuai, dan daftar pelanggan hanya berisi pengguna yang diizinkan untuk melihat informasi tentang sumber daya. Jika topik Amazon SNS adalah topik yang digunakan untuk CodeCommit pemberitahuan sebelum 5 November 2019, itu akan berisi kebijakan yang memungkinkan CodeCommit untuk mempublikasikannya yang berisi izin berbeda dari yang diperlukan untuk Pemberitahuan. AWS CodeStar Menggunakan topik ini tidak disarankan. Jika Anda ingin menggunakan yang dibuat untuk pengalaman itu, Anda harus menambahkan kebijakan yang diperlukan untuk AWS CodeStar Pemberitahuan selain yang sudah ada. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) dan [Memahami konten dan keamanan notifikasi](#).

8. Pilih Kirim, dan kemudian tinjau aturan notifikasi.
9. Berlangganan alamat email Anda ke topik Amazon SNS yang baru saja Anda buat. Untuk informasi lebih lanjut, lihat [Untuk berlangganan pengguna ke topik Amazon SNS yang digunakan untuk notifikasi](#).
10. Arahkan ke aplikasi deployment Anda dan mulai deployment.
11. Setelah deployment berhasil, aturan notifikasi mengirimkan notifikasi ke semua pelanggan topik dengan informasi tentang acara tersebut.

Membuat aturan notifikasi untuk alur

Anda dapat membuat aturan notifikasi untuk mengirim notifikasi tentang peristiwa pada alur yang penting bagi Anda. Langkah-langkah berikut menunjukkan cara mengatur aturan notifikasi pada peristiwa alur tunggal. Langkah-langkah ini ditulis dengan asumsi bahwa Anda memiliki pipeline yang dikonfigurasi di AWS akun Anda.

1. Buka CodePipeline konsol di <https://console.aws.amazon.com/codepipeline/>.
2. Pilih alur dari daftar dan buka.
3. Pilih Beri tahu, lalu pilih Buat aturan notifikasi. Anda juga dapat memilih Pengaturan, lalu pilih Buat aturan notifikasi.
4. Di Nama notifikasi, masukkan nama untuk aturan.
5. Di Jenis detail, pilih Dasar jika Anda hanya menginginkan informasi yang diberikan ke Amazon yang EventBridge disertakan dalam notifikasi. Pilih Lengkap jika Anda ingin menyertakan informasi yang diberikan ke Amazon EventBridge dan informasi yang mungkin disediakan oleh layanan sumber daya atau pengelola notifikasi.

Untuk informasi selengkapnya, lihat [Memahami konten dan keamanan notifikasi](#).

6. Di Peristiwa yang memicu notifikasi, di bawah Eksekusi tindakan, pilih Dimulai.
7. Di Target, pilih Buat topik SNS.

Note

Saat Anda membuat topik sebagai bagian dari pembuatan aturan notifikasi, kebijakan yang memungkinkan CodePipeline untuk mempublikasikan peristiwa ke topik diterapkan untuk Anda. Menggunakan topik yang dibuat untuk aturan notifikasi membantu memastikan bahwa Anda hanya berlangganan hanya pada pengguna yang ingin Anda terima notifikasinya tentang alur ini.

Setelah prefiks `codestar-notifications-`, masukkan nama untuk topik, lalu pilih nama, lalu pilih Kirim.

Note

Jika Anda ingin menggunakan topik Amazon SNS yang sudah ada alih-alih membuat yang baru, di Target, pilih ARN-nya. Pastikan topik memiliki kebijakan akses yang

sesuai, dan daftar pelanggan hanya berisi pengguna yang diizinkan untuk melihat informasi tentang sumber daya. Jika topik Amazon SNS adalah topik yang digunakan untuk CodeCommit pemberitahuan sebelum 5 November 2019, itu akan berisi kebijakan yang memungkinkan CodeCommit untuk mempublikasikannya yang berisi izin berbeda dari yang diperlukan untuk Pemberitahuan. AWS CodeStar Menggunakan topik ini tidak disarankan. Jika Anda ingin menggunakan yang dibuat untuk pengalaman itu, Anda harus menambahkan kebijakan yang diperlukan untuk AWS CodeStar Pemberitahuan selain yang sudah ada. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) dan [Memahami konten dan keamanan notifikasi](#).

8. Pilih Kirim, dan kemudian tinjau aturan notifikasi.
9. Berlangganan alamat email Anda ke topik Amazon SNS yang baru saja Anda buat. Untuk informasi lebih lanjut, lihat [Untuk berlangganan pengguna ke topik Amazon SNS yang digunakan untuk notifikasi](#).
10. Arahkan ke alur Anda, lalu pilih Perubahan rilis.
11. Ketika tindakan dimulai, aturan notifikasi mengirimkan notifikasi ke semua pelanggan topik dengan informasi tentang acara tersebut.

Bekerja dengan aturan notifikasi

Aturan notifikasi adalah tempat Anda mengonfigurasi acara mana yang Anda inginkan pengguna untuk menerima notifikasi tentang dan menentukan target yang menerima notifikasi tersebut. Anda dapat mengirim notifikasi langsung ke pengguna melalui Amazon SNS, atau melalui klien Chatbot yang dikonfigurasi untuk AWS saluran Slack atau Microsoft Teams. Jika Anda ingin memperluas jangkauan notifikasi, Anda dapat mengonfigurasi integrasi antara notifikasi dan AWS Chatbot secara manual sehingga notifikasi dikirim ke ruang obrolan Amazon Chime. Untuk informasi selengkapnya, lihat [Target](#) dan [Untuk mengintegrasikan notifikasi dengan AWS Chatbot dan Amazon Chime](#).

Create notification rule

Notification rules set up a subscription to events that happen with your resources. When these events occur, you will receive notifications sent to the targets you designate. You can manage your notification preferences in Settings. [Info](#)

Notification rule settings

Notification name

Detail type

Choose the level of detail you want in notifications. [Learn more about notifications and security](#)

Full

Includes any supplemental information about events provided by the resource or the notifications feature.

Basic

Includes only information provided in resource events.

Events that trigger notifications

Comments

- On commits
- On pull requests

Approvals

- Status changed
- Rule override

Pull request

- Source updated
- Created
- Status changed
- Merged

Branches and tags

- Created
- Deleted
- Updated

Targets

Choose a target type for the notification rule. SNS topics can be created specifically for use with the notification rule, or existing topics can be modified for use with notifications. AWS Chatbot clients for Slack integration must be created before you can choose them as a target type. [Learn more](#)

Anda dapat menggunakan konsol Alat Pengembang atau AWS CLI untuk membuat dan mengelola aturan notifikasi.

Topik

- [Membuat aturan notifikasi](#)

- [Lihat aturan notifikasi](#)
- [Mengedit aturan notifikasi](#)
- [Mengaktifkan atau menonaktifkan notifikasi untuk aturan notifikasi](#)
- [Menghapus aturan notifikasi](#)

Membuat aturan notifikasi

Anda dapat menggunakan konsol Alat Pengembang atau AWS CLI untuk membuat aturan pemberitahuan. Anda dapat membuat untuk membuat topik Amazon SNS untuk digunakan sebagai target sebagai bagian dari pembuatan aturan. Jika Anda ingin menggunakan klien AWS Chatbot sebagai target, Anda harus membuat klien itu sebelum Anda dapat membuat aturan. Untuk informasi selengkapnya, lihat [Konfigurasi klien AWS Chatbot untuk saluran Slack](#).

Untuk membuat aturan notifikasi (konsol)

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Gunakan bilah navigasi untuk menavigasi ke sumber daya.
 - Untuk CodeBuild, pilih Build, pilih Build projects, dan pilih build project.
 - Untuk CodeCommit, pilih Sumber, pilih Repositori, dan pilih repositori.
 - Untuk CodeDeploy, pilih Aplikasi, dan pilih aplikasi.
 - Untuk CodePipeline, pilih Pipeline, pilih Pipelines, dan pilih pipeline.
3. Pada halaman sumber daya, pilih Beri tahu, lalu pilih Buat aturan notifikasi. Anda juga dapat masuk ke halaman Pengaturan untuk sumber daya, masuk ke Notifikasi atau Aturan notifikasi, lalu pilih Membuat aturan notifikasi.
4. Di Nama notifikasi, masukkan nama untuk aturan.
5. Di Jenis detail, pilih Dasar jika Anda hanya menginginkan informasi yang diberikan ke Amazon yang EventBridge disertakan dalam notifikasi. Pilih Lengkap jika Anda ingin menyertakan informasi yang diberikan ke Amazon EventBridge dan informasi yang mungkin disediakan oleh layanan sumber daya atau pengelola notifikasi.


Untuk informasi selengkapnya, lihat [Memahami konten dan keamanan notifikasi](#).

6. Di Peristiwa yang memicu notifikasi, pilih peristiwa yang ingin Anda kirimkan notifikasi. Untuk jenis peristiwa untuk sumber daya, lihat berikut ini:

- CodeBuild: [Acara untuk aturan notifikasi tentang proyek build](#)
- CodeCommit: [Peristiwa untuk aturan notifikasi pada repositori](#)
- CodeDeploy: [Peristiwa untuk aturan notifikasi pada aplikasi deployment](#)
- CodePipeline: [Acara untuk aturan notifikasi pada alur](#)


7. Di Target, lakukan salah satu langkah berikut:

- Jika Anda telah mengonfigurasi sumber daya untuk digunakan dengan notifikasi, di Pilih jenis target, pilih AWS Chatbot (Slack), Chatbot AWS (Microsoft Teams), atau topik SNS. Di Pilih target, pilih nama klien (untuk klien Slack atau Microsoft Teams yang dikonfigurasi di AWS Chatbot) atau Nama Sumber Daya Amazon (ARN) dari topik Amazon SNS (untuk topik Amazon SNS yang sudah dikonfigurasi dengan kebijakan yang diperlukan untuk pemberitahuan).
- Jika Anda belum mengonfigurasi sumber daya untuk digunakan dengan notifikasi, pilih Buat target, lalu pilih Topik SNS. Berikan nama untuk topik setelah codestar-notifications-, lalu pilih Buat.

 Note

- Jika Anda membuat topik Amazon SNS sebagai bagian dari membuat aturan notifikasi, kebijakan yang memungkinkan fitur notifikasi untuk mempublikasikan peristiwa untuk topik diterapkan untuk Anda. Menggunakan topik yang dibuat untuk aturan notifikasi membantu memastikan bahwa Anda hanya berlangganan pengguna yang ingin Anda terima notifikasinya tentang sumber daya ini.
- Anda tidak dapat membuat klien AWS Chatbot sebagai bagian dari pembuatan aturan notifikasi. Jika Anda memilih AWS Chatbot (Slack) atau Chatbot AWS (Microsoft Teams), Anda akan melihat tombol yang mengarahkan Anda untuk mengonfigurasi klien di Chatbot. AWS Memilih opsi itu membuka konsol AWS Chatbot. Untuk informasi selengkapnya, lihat [Konfigurasi klien AWS Chatbot untuk saluran Slack](#).
- Jika ingin menggunakan topik Amazon SNS yang ada sebagai target, Anda harus menambahkan kebijakan yang diperlukan untuk AWS CodeStar Pemberitahuan selain kebijakan lain yang mungkin ada untuk topik tersebut. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) dan [Memahami konten dan keamanan notifikasi](#).

- Pilih Kirim, dan kemudian tinjau aturan notifikasi.

 Note

Pengguna harus berlangganan dan mengonfirmasi langganan ke topik Amazon SNS yang Anda tentukan sebagai target aturan sebelum mereka akan menerima notifikasi. Untuk informasi lebih lanjut, lihat [Untuk berlangganan pengguna ke topik Amazon SNS yang digunakan untuk notifikasi](#).

Membuat aturan notifikasi (AWS CLI)

- Di terminal atau permintaan perintah, jalankan perintah `create-notification rule` untuk menghasilkan kerangka JSON.

```
aws codestar-notifications create-notification-rule --generate-cli-skeleton  
> rule.json
```

Anda dapat memberi nama file apa pun yang Anda inginkan. Dalam contoh ini, file dinamai *rule.json*.

- Buka file JSON dalam editor plaintext dan edit untuk memasukkan sumber daya, jenis peristiwa, dan target Amazon SNS yang Anda inginkan untuk aturan.

Contoh berikut menunjukkan aturan notifikasi bernama **MyNotificationRule** untuk repositori bernama *MyDemoRepo* dalam AWS akun dengan ID. *123456789012* Pemberitahuan dengan tipe detail lengkap dikirim ke topik Amazon SNS yang diberi nama *MyNotificationTopic* saat cabang dan tag dibuat.

```
{  
  "Name": "MyNotificationRule",  
  "EventTypeIds": [  
    "codecommit-repository-branches-and-tags-created"  
  ],  
  "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",  
  "Targets": [  
    {  
      "TargetType": "SNS",
```

```

      "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic"
    }
  ],
  "Status": "ENABLED",
  "DetailType": "FULL"
}

```

Simpan file tersebut.

3. Menggunakan file yang baru saja Anda edit, di terminal atau baris perintah, jalankan perintah `create-notification-rule` kembali untuk membuat aturan notifikasi.

```

aws codestar-notifications create-notification-rule --cli-input-json
file://rule.json

```

4. Jika berhasil, perintah mengembalikan ARN aturan notifikasi, mirip dengan berikut ini.

```

{
  "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}

```

Untuk mencantumkan jenis peristiwa untuk aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah `list-event-types`. Anda dapat menggunakan pilihan `--filters` untuk membatasi respons ke jenis sumber daya tertentu atau atribut lainnya. Misalnya, berikut ini mengembalikan daftar jenis acara untuk CodeDeploy aplikasi.

```

aws codestar-notifications list-event-types --filters
Name=SERVICE_NAME,Value=CodeDeploy

```

2. Perintah ini menghasilkan output seperti berikut.

```

{
  "EventTypes": [
    {
      "EventTypeId": "codedeploy-application-deployment-succeeded",
      "ServiceName": "CodeDeploy",
      "EventTypeName": "Deployment: Succeeded",

```

```

    "ResourceType": "Application"
  },
  {
    "EventTypeId": "codedeploy-application-deployment-failed",
    "ServiceName": "CodeDeploy",
    "EventTypeName": "Deployment: Failed",
    "ResourceType": "Application"
  },
  {
    "EventTypeId": "codedeploy-application-deployment-started",
    "ServiceName": "CodeDeploy",
    "EventTypeName": "Deployment: Started",
    "ResourceType": "Application"
  }
]
}

```

Untuk menambahkan tanda ke aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah `tag-resource`. Misalnya, gunakan perintah berikut untuk menambahkan pasangan nilai kunci tag yang memiliki nama *Team* dan nilainya.

Li_Juan

```
aws codestar-notifications tag-resource --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/fe1efd35-EXAMPLE --tags Team=Li_Juan
```

2. Perintah ini menghasilkan output seperti berikut.

```
{
  "Tags": {
    "Team": "Li_Juan"
  }
}
```

Lihat aturan notifikasi

Anda dapat menggunakan konsol Alat Pengembang atau AWS CLI untuk melihat semua aturan pemberitahuan untuk semua sumber daya di AWS Wilayah. Anda juga dapat melihat detail setiap aturan notifikasi. Tidak seperti proses untuk membuat aturan notifikasi, Anda tidak perlu pergi ke halaman sumber daya untuk sumber daya.

Untuk melihat aturan notifikasi (konsol)

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Di bilah navigasi, perluas Pengaturan, lalu pilih Aturan notifikasi.
3. Dalam aturan Pemberitahuan, tinjau daftar aturan yang dikonfigurasi untuk sumber daya Anda Akun AWS di Wilayah AWS tempat Anda saat ini masuk. Gunakan pemilih untuk mengubah Wilayah AWS
4. Untuk melihat detail aturan notifikasi, pilih dari daftar, lalu pilih Lihat detail. Anda juga bisa memilih namanya di daftar.

Untuk melihat daftar aturan notifikasi (AWS CLI)

1. Pada terminal atau command prompt, jalankan list-notification-rules perintah untuk melihat semua aturan notifikasi untuk AWS Wilayah yang ditentukan.

```
aws codestar-notifications list-notification-rules --region us-east-1
```

2. Jika berhasil, perintah ini mengembalikan ID dan ARN untuk setiap aturan notifikasi di AWS Wilayah, mirip dengan yang berikut ini.

```
{
  "NotificationRules": [
    {
      "Id": "dc82df7a-EXAMPLE",
      "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE"
    },
    {
      "Id": "8d1f0983-EXAMPLE",
      "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/8d1f0983-EXAMPLE"
    }
  ]
}
```

Untuk melihat detail aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah `describe-notification-rule`, menentukan ARN aturan notifikasi.

```
aws codestar-notifications describe-notification-rule --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE
```

2. Jika berhasil, perintah mengembalikan output yang serupa dengan yang berikut.

```
{
  "LastModifiedTimestamp": 1569199844.857,
  "EventTypes": [
    {
      "ServiceName": "CodeCommit",
      "EventTypeName": "Branches and tags: Created",
      "ResourceType": "Repository",
      "EventTypeId": "codecommit-repository-branches-and-tags-created"
    }
  ],
  "Status": "ENABLED",
  "DetailType": "FULL",
  "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
  "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE",
  "Targets": [
    {
      "TargetStatus": "ACTIVE",
      "TargetAddress": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopic",
      "TargetType": "SNS"
    }
  ],
  "Name": "MyNotificationRule",
  "CreatedTimestamp": 1569199844.857,
  "CreatedBy": "arn:aws:iam::123456789012:user/Mary_Major"
}
```

Untuk melihat daftar tanda untuk aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah `list-tags-for-resource` untuk melihat semua tanda untuk ARN aturan notifikasi tertentu.

```
aws codestar-notifications list-tags-for-resource --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/fe1efd35-EXAMPLE
```

2. Jika berhasil, perintah ini mengembalikan output yang serupa dengan yang berikut.

```
{
  "Tags": {
    "Team": "Li_Juan"
  }
}
```

Mengedit aturan notifikasi

Anda dapat mengedit aturan notifikasi untuk mengubah namanya, peristiwa yang mengirimkan notifikasi, jenis detail, atau target atau target yang mengirimkan notifikasi. Anda dapat menggunakan konsol Alat Pengembang atau AWS CLI untuk mengedit aturan pemberitahuan.

Untuk mengedit aturan notifikasi (konsol)

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Di bilah navigasi, perluas Pengaturan, lalu pilih Aturan notifikasi.
3. Dalam aturan Pemberitahuan, tinjau aturan yang dikonfigurasi untuk sumber daya di AWS akun Wilayah AWS di tempat Anda saat ini masuk. Gunakan pemilih untuk mengubah Wilayah AWS.
4. Pilih aturan dari daftar, lalu pilih Edit. Lakukan perubahan, dan pilih Kirim.

Untuk mengedit aturan notifikasi (AWS CLI)

1. Pada terminal atau command prompt, jalankan [describe-notification-ruleperintah](#) untuk melihat struktur aturan notifikasi.
2. Jalankan perintah `update-notification rule` untuk menghasilkan kerangka JSON dan kemudian menyimpannya ke file.

```
aws codestar-notifications update-notification-rule --generate-cli-skeleton  
> update.json
```

Anda dapat memberi nama file apa pun yang Anda inginkan. Dalam contoh ini, file tersebut adalah *update.json*.

3. Buka file JSON dalam editor plaintext dan buat perubahan aturan.

Contoh berikut menunjukkan aturan notifikasi bernama **MyNotificationRule** untuk repositori bernama *MyDemoRepo* dalam AWS akun dengan ID. *123456789012* Pemberitahuan dikirim ke topik Amazon SNS yang diberi nama *MyNotificationTopic* saat cabang dan tag dibuat. Nama aturan diubah menjadi *MyNewNotificationRule*.

```
{  
  "Name": "MyNewNotificationRule",  
  "EventIds": [  
    "codecommit-repository-branches-and-tags-created"  
  ],  
  "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",  
  "Targets": [  
    {  
      "TargetType": "SNS",  
      "TargetAddress": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopic"  
    }  
  ],  
  "Status": "ENABLED",  
  "DetailType": "FULL"  
}
```

Simpan file tersebut.

4. Menggunakan file yang baru saja Anda edit, di terminal atau baris perintah, jalankan perintah `update-notification-rule` lagi untuk memperbarui aturan notifikasi.

```
aws codestar-notifications update-notification-rule --cli-input-json  
file://update.json
```

5. Jika berhasil, perintah mengembalikan Amazon Resource Name (ARN) dari aturan notifikasi, mirip dengan berikut ini.

```
{
  "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Untuk menghapus tanda dari aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah `untag-resource`. Misalnya, perintah berikut menghapus tag dengan nama *Team*.

```
aws codestar-notifications untag-resource --arn arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/fe1efd35-EXAMPLE --tag-keys Team
```

2. Jika berhasil, perintah ini tidak mengembalikan apa pun.

Lihat juga

- [Menambah atau menghapus target untuk aturan notifikasi](#)
- [Mengaktifkan atau menonaktifkan notifikasi untuk aturan notifikasi](#)
- [Peristiwa](#)

Mengaktifkan atau menonaktifkan notifikasi untuk aturan notifikasi

Saat Anda membuat aturan notifikasi, notifikasi diaktifkan secara default. Anda tidak harus menghapus aturan untuk mencegahnya mengirim notifikasi. Anda cukup mengubah status notifikasinya.

Untuk mengubah status notifikasi untuk aturan notifikasi (konsol)

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Di bilah navigasi, perluas Pengaturan, lalu pilih Aturan notifikasi.
3. Dalam aturan Pemberitahuan, tinjau aturan yang dikonfigurasi untuk sumber daya di AWS akun Wilayah AWS di tempat Anda saat ini masuk. Gunakan pemilih untuk mengubah Wilayah AWS.
4. Temukan aturan notifikasi yang ingin Anda aktifkan atau nonaktifkan, lalu pilih untuk menampilkan detailnya.

5. Di Status notifikasi, pilih slider untuk mengubah status aturan:

- Mengirim notifikasi: Ini adalah pengaturan default.
- Notifikasi dijeda: Tidak ada notifikasi dikirim ke target yang ditentukan.

Untuk mengubah status notifikasi untuk aturan notifikasi (AWS CLI)

1. Ikuti langkah-langkah di [Untuk mengedit aturan notifikasi \(AWS CLI\)](#) untuk mendapatkan JSON untuk aturan notifikasi.
2. Edit bidang Status ke ENABLED(default) atau DISABLED (tidak ada notifikasi), dan kemudian jalankan perintah update-notification-rule untuk mengubah status.

```
"Status": "ENABLED"
```

Menghapus aturan notifikasi

Hanya ada 10 aturan notifikasi yang dikonfigurasi untuk sumber daya, jadi pertimbangkan untuk menghapus aturan yang tidak diperlukan lagi. Anda dapat menggunakan konsol Alat Pengembang atau AWS CLI untuk menghapus aturan pemberitahuan.

Note

Anda tidak dapat membatalkan penghapusan aturan notifikasi, tetapi Anda dapat membuatnya kembali. Menghapus aturan notifikasi tidak menghapus target.

Untuk menghapus aturan notifikasi (konsol)

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Di bilah navigasi, perluas Pengaturan, lalu pilih Aturan notifikasi.
3. Dalam aturan Pemberitahuan, tinjau aturan yang dikonfigurasi untuk sumber daya di AWS akun Wilayah AWS di tempat Anda saat ini masuk. Gunakan pemilih untuk mengubah. Wilayah AWS
4. Pilih aturan notifikasi, dan kemudian pilih Hapus.
5. Ketik **delete**, lalu pilih Hapus.

Untuk menghapus aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah `delete-notification-rule`, tentukan ARN aturan notifikasi.

```
aws codestar-notifications delete-notification-rule --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE
```

2. Jika berhasil, perintah mengembalikan ARN aturan notifikasi yang dihapus, mirip dengan berikut ini.

```
{
  "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE"
}
```

Bekerja dengan target aturan notifikasi

Target aturan notifikasi adalah tujuan yang menentukan di mana Anda ingin notifikasi dikirim ketika kondisi peristiwa aturan notifikasi terpenuhi. Anda dapat memilih antara topik Amazon SNS dan klien Chatbot AWS yang dikonfigurasi untuk saluran Slack atau Microsoft Teams. Anda dapat membuat topik Amazon SNS sebagai target sebagai bagian dari pembuatan aturan notifikasi (disarankan). Anda juga dapat memilih topik Amazon SNS yang ada di AWS Wilayah yang sama dengan aturan notifikasi, tetapi Anda harus mengonfigurasinya dengan kebijakan yang diperlukan. Jika Anda memilih untuk menggunakan klien AWS Chatbot sebagai target, Anda harus terlebih dahulu membuat klien itu di AWS Chatbot.

Jika Anda ingin memperluas jangkauan notifikasi, Anda dapat mengonfigurasi integrasi antara notifikasi dan AWS Chatbot secara manual sehingga notifikasi dikirim ke ruang obrolan Amazon Chime. Anda kemudian dapat memilih topik Amazon SNS yang dikonfigurasi untuk klien Chatbot AWS tersebut sebagai target untuk aturan notifikasi. Untuk informasi selengkapnya, lihat [Untuk mengintegrasikan notifikasi dengan AWS Chatbot dan Amazon Chime](#).

Anda dapat menggunakan konsol Alat Pengembang atau AWS CLI untuk mengelola target notifikasi. [Anda dapat menggunakan konsol atau AWS CLI untuk membuat dan mengonfigurasi topik Amazon SNS dan klien Chatbot sebagai AWS target](#). Anda juga dapat mengonfigurasi integrasi antara topik Amazon SNS yang Anda konfigurasi sebagai target dan AWS Chatbot. Hal ini memungkinkan

Anda untuk mengirim notifikasi ke ruang obrolan Amazon Chime. Untuk informasi lebih lanjut, lihat [Konfigurasi integrasi antara notifikasi dan AWS Chatbot](#).

Topik

- [Membuat atau mengonfigurasi target aturan notifikasi](#)
- [Lihat target aturan notifikasi](#)
- [Menambah atau menghapus target untuk aturan notifikasi](#)
- [Menghapus target aturan notifikasi](#)

Membuat atau mengonfigurasi target aturan notifikasi

Target aturan notifikasi adalah topik Amazon SNS atau klien Chatbot yang dikonfigurasi untuk AWS saluran Slack atau Microsoft Teams.

Klien AWS Chatbot harus dibuat sebelum Anda dapat memilih klien sebagai target. Saat Anda memilih klien AWS Chatbot sebagai target untuk aturan notifikasi, topik Amazon SNS dikonfigurasi untuk klien AWS Chatbot tersebut dengan semua kebijakan yang diperlukan agar notifikasi dikirim ke saluran Slack atau Microsoft Teams. Anda tidak perlu mengonfigurasi topik Amazon SNS yang ada untuk klien Chatbot AWS .

Anda dapat membuat target aturan notifikasi Amazon SNS di konsol Alat Developer ketika Anda membuat aturan notifikasi. Kebijakan yang memungkinkan notifikasi dikirim ke topik tersebut diterapkan untuk Anda. Ini adalah cara termudah untuk membuat target untuk aturan notifikasi. Untuk informasi lebih lanjut, lihat [Membuat aturan notifikasi](#).

Jika Anda menggunakan topik Amazon SNS yang sudah ada, Anda harus mengonfigurasi dengan kebijakan akses yang memungkinkan sumber daya untuk mengirim notifikasi ke topik tersebut. Sebagai contoh, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#).

Note

Jika Anda ingin menggunakan topik Amazon SNS yang sudah ada alih-alih membuat yang baru, di Target, pilih ARN-nya. Pastikan topik memiliki kebijakan akses yang sesuai, dan daftar pelanggan hanya berisi pengguna yang diizinkan untuk melihat informasi tentang sumber daya. Jika topik Amazon SNS adalah topik yang digunakan untuk CodeCommit pemberitahuan sebelum 5 November 2019, itu akan berisi kebijakan yang memungkinkan CodeCommit untuk mempublikasikannya yang berisi izin berbeda dari yang diperlukan untuk Pemberitahuan. AWS CodeStar Menggunakan topik ini tidak disarankan. Jika Anda ingin

menggunakan yang dibuat untuk pengalaman itu, Anda harus menambahkan kebijakan yang diperlukan untuk AWS CodeStar Pemberitahuan selain yang sudah ada. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) dan [Memahami konten dan keamanan notifikasi](#).

Jika Anda ingin memperluas jangkauan notifikasi, Anda dapat mengonfigurasi integrasi antara notifikasi dan AWS Chatbot secara manual sehingga notifikasi dikirim ke ruang obrolan Amazon Chime. Untuk informasi selengkapnya, lihat [Target](#) dan [Untuk mengintegrasikan notifikasi dengan AWS Chatbot dan Amazon Chime](#).

Untuk mengonfigurasi topik Amazon SNS yang ada untuk digunakan sebagai target aturan notifikasi (konsol)

1. [Masuk ke Konsol Manajemen AWS dan buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Di bilah navigasi, pilih Topik. Pilih topik, dan kemudian pilih Edit.
3. Perluas Kebijakan akses, lalu pilih Lanjutan.
4. Pada editor JSON, tambahkan pernyataan berikut ke kebijakan. Sertakan topik ARN,, Akun AWS ID Wilayah AWS, dan nama topik.

```
{
  "Sid": "AWSCodeStarNotifications_publish",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "codestar-notifications.amazonaws.com"
    ]
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-MyTopicForNotificationRules"
}
```

Pernyataan kebijakan akan terlihat seperti berikut.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
```

```

"Statement": [
  {
    "Sid": "__default_statement_ID",
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": [
      "SNS:GetTopicAttributes",
      "SNS:SetTopicAttributes",
      "SNS:AddPermission",
      "SNS:RemovePermission",
      "SNS:DeleteTopic",
      "SNS:Subscribe",
      "SNS:ListSubscriptionsByTopic",
      "SNS:Publish"
    ],
    "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-MyTopicForNotificationRules",
    "Condition": {
      "StringEquals": {
        "AWS:SourceOwner": "123456789012"
      }
    }
  },
  {
    "Sid": "AWSCodeStarNotifications_publish",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "codestar-notifications.amazonaws.com"
      ]
    },
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:us-east-2:123456789012:codestar-notifications-MyTopicForNotificationRules"
  }
]
}


```

5. Pilih Simpan perubahan.
6. Di Langganan, tinjau daftar pelanggan topik. Menambahkan, mengedit, atau menghapus pelanggan yang sesuai untuk target aturan notifikasi ini. Pastikan bahwa daftar pelanggan hanya

berisi pengguna yang diizinkan untuk melihat informasi tentang sumber daya. Untuk informasi selengkapnya, lihat [Memahami konten dan keamanan notifikasi](#).

Untuk membuat klien AWS Chatbot dengan Slack untuk digunakan sebagai target

1. Ikuti petunjuk dalam [Menyiapkan AWS Chatbot dengan Slack](#) di Panduan Administrator Chatbot AWS . Apabila Anda melakukannya, pertimbangkan pilihan berikut untuk integrasi optimum dengan notifikasi:
 - Saat membuat IAM role, pertimbangkan untuk memilih nama peran yang memudahkan untuk mengidentifikasi tujuan peran ini (misalnya, **AWSCodeStarNotifications-Chatbot-Slack-Role**). Ini dapat membantu Anda mengidentifikasi tujuan peran di masa depan.
 - Dalam topik SNS, Anda tidak harus memilih topik atau AWS Wilayah. Saat Anda memilih klien AWS Chatbot sebagai [target](#), topik Amazon SNS dengan semua izin yang diperlukan dibuat dan dikonfigurasi untuk klien AWS Chatbot sebagai bagian dari proses pembuatan aturan notifikasi.
2. Menyelesaikan proses pembuatan klien. Klien ini kemudian tersedia bagi Anda untuk memilih sebagai target saat membuat aturan notifikasi. Untuk informasi selengkapnya, lihat [Membuat aturan notifikasi](#).

 Note

Jangan hapus topik Amazon SNS dari klien Chatbot AWS setelah dikonfigurasi untuk Anda. Melakukan hal tersebut akan mencegah notifikasi dikirim ke Slack.

Untuk membuat klien AWS Chatbot dengan Microsoft Teams untuk digunakan sebagai target

1. Ikuti petunjuk dalam [Menyiapkan AWS Chatbot dengan Microsoft Teams di Panduan Administrator](#) Chatbot AWS . Apabila Anda melakukannya, pertimbangkan pilihan berikut untuk integrasi optimum dengan notifikasi:
 - Saat membuat IAM role, pertimbangkan untuk memilih nama peran yang memudahkan untuk mengidentifikasi tujuan peran ini (misalnya, **AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role**). Ini dapat membantu Anda mengidentifikasi tujuan peran di masa depan.

- Dalam topik SNS, Anda tidak harus memilih topik atau AWS Wilayah. Saat Anda memilih klien AWS Chatbot sebagai [target](#), topik Amazon SNS dengan semua izin yang diperlukan dibuat dan dikonfigurasi untuk klien AWS Chatbot sebagai bagian dari proses pembuatan aturan notifikasi.
2. Menyelesaikan proses pembuatan klien. Klien ini kemudian tersedia bagi Anda untuk memilih sebagai target saat membuat aturan notifikasi. Untuk informasi selengkapnya, lihat [Membuat aturan notifikasi](#).

Note

Jangan hapus topik Amazon SNS dari klien Chatbot AWS setelah dikonfigurasi untuk Anda. Melakukannya akan mencegah pemberitahuan dikirim ke Microsoft Teams.

Lihat target aturan notifikasi

Anda dapat menggunakan konsol Alat Pengembang, bukan konsol Amazon SNS untuk melihat semua target aturan notifikasi untuk semua sumber daya di Wilayah. AWS Anda juga dapat melihat detail target aturan notifikasi.

Untuk melihat target aturan notifikasi (konsol)

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Di bilah navigasi, perluas Pengaturan, lalu pilih Aturan notifikasi.
3. Di Target aturan Pemberitahuan, tinjau daftar target yang digunakan oleh aturan notifikasi Akun AWS di Wilayah AWS tempat Anda saat ini masuk. Gunakan pemilih untuk mengubah Wilayah AWS. Jika status target menunjukkan sebagai Tidak terjangkau, Anda mungkin perlu menyelidiki. Untuk informasi selengkapnya, lihat [Pemecahan Masalah](#).

Untuk melihat daftar target aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah `list-targets` untuk melihat daftar semua target aturan notifikasi untuk Wilayah AWS :

```
aws codestar-notifications list-targets --region us-east-2
```

2. Jika berhasil, perintah ini mengembalikan ID dan ARN untuk setiap aturan notifikasi di AWS Wilayah, mirip dengan yang berikut ini:

```
{
  "Targets": [
    {
      "TargetAddress": "arn:aws:sns:us-
east-2:123456789012:MySNSTopicForNotificationRules",
      "TargetType": "SNS",
      "TargetStatus": "ACTIVE"
    },
    {
      "TargetAddress": "arn:aws:chatbot::123456789012:chat-configuration/
slack-channel/MySlackChannelClientForMyDevTeam",
      "TargetStatus": "ACTIVE",
      "TargetType": "AWSChatbotSlack"
    },
    {
      "TargetAddress": "arn:aws:sns:us-
east-2:123456789012:MySNSTopicForNotificationsAboutMyDemoRepo",
      "TargetType": "SNS",
      "TargetStatus": "ACTIVE"
    }
  ]
}
```

Menambah atau menghapus target untuk aturan notifikasi

Anda dapat mengedit aturan notifikasi untuk mengubah target atau target yang mengirimkan notifikasi. Anda dapat menggunakan konsol Alat Pengembang atau atau AWS CLI untuk mengubah target aturan pemberitahuan.

Untuk mengubah target untuk aturan notifikasi (konsol)

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Di bilah navigasi, perluas Pengaturan, lalu pilih Aturan notifikasi.
3. Dalam aturan Pemberitahuan, tinjau daftar aturan yang dikonfigurasi untuk sumber daya Anda di AWS akun Wilayah AWS di tempat Anda saat ini masuk. Gunakan pemilih untuk mengubah Wilayah AWS

4. Pilih aturan, dan kemudian pilih Edit.
5. Di Target, lakukan salah satu langkah berikut:
 - Untuk menambahkan target lain, pilih Tambahkan Target, lalu pilih topik Amazon SNS atau AWS Chatbot (Slack) atau klien AWS Chatbot (Microsoft Teams) yang ingin Anda tambahkan dari daftar. Anda juga dapat memilih Buat topik SNS untuk membuat topik dan menambahkannya sebagai target. Aturan notifikasi dapat memiliki hingga 10 target.
 - Untuk menghapus target, di samping target yang ingin dihapus, pilih Hapus target.
6. Pilih Kirim.

Untuk menambahkan target ke aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah subscribe untuk menambahkan target. Sebagai contoh, perintah berikut menambahkan topik Amazon SNS sebagai target untuk aturan notifikasi.

```
aws codestar-notifications subscribe --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-
EXAMPLE --target TargetType=SNS,TargetAddress=arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic
```

2. Jika berhasil, perintah mengembalikan ARN aturan notifikasi yang diperbarui, mirip dengan berikut ini.

```
{
  "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Untuk menghapus target dari aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah unsubscribe untuk menghapus target. Sebagai contoh, perintah berikut menghapus topik Amazon SNS sebagai target untuk aturan notifikasi.

```
aws codestar-notifications unsubscribe --arn arn:aws:codestar-
notifications:us-east-1:123456789012:notificationrule/dc82df7a-
```

```
EXAMPLE --target TargetType=SNS,TargetAddress=arn:aws:sns:us-east-1:123456789012:MyNotificationTopic
```

2. Jika berhasil, perintah mengembalikan ARN aturan notifikasi diperbarui dan informasi tentang target dihapus, mirip dengan berikut ini.

```
{
  "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE"
  "TargetAddress": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopic"
}
```

Lihat juga

- [Mengedit aturan notifikasi](#)
- [Mengaktifkan atau menonaktifkan notifikasi untuk aturan notifikasi](#)

Menghapus target aturan notifikasi

Anda dapat menghapus target jika tidak lagi diperlukan. Sumber daya hanya dapat memiliki 10 target aturan notifikasi yang dikonfigurasi untuk itu, sehingga menghapus target yang tidak diperlukan dapat membantu menciptakan ruang untuk target lain yang mungkin ingin Anda tambahkan ke aturan notifikasi tersebut.

Note

Menghapus target aturan notifikasi berarti menghapus target dari semua aturan notifikasi yang dikonfigurasi untuk digunakan sebagai target, tetapi tidak menghapus target itu sendiri.

Untuk menghapus target aturan notifikasi (konsol)

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Di bilah navigasi, perluas Pengaturan, lalu pilih Aturan notifikasi.
3. Di Target aturan Pemberitahuan, tinjau daftar target yang dikonfigurasi untuk sumber daya Anda di AWS akun Wilayah AWS di tempat Anda saat ini masuk. Gunakan pemilih untuk mengubah Wilayah AWS

4. Pilih target aturan notifikasi, dan kemudian pilih Hapus.
5. Ketik **delete**, lalu pilih Hapus.

Untuk menghapus target aturan notifikasi (AWS CLI)

1. Di terminal atau permintaan perintah, jalankan perintah `delete-target`, tentukan ARN target. Sebagai contoh, perintah berikut menghapus target yang menggunakan topik Amazon SNS.

```
aws codestar-notifications delete-target --target-address arn:aws:sns:us-east-1:123456789012:MyNotificationTopic
```

2. Jika berhasil, perintah tidak mengembalikan apa pun. Jika tidak berhasil, perintah mengembalikan kesalahan. Kesalahan yang paling umum adalah bahwa topik adalah target untuk satu atau lebih aturan notifikasi.

```
An error occurred (ValidationException) when calling the DeleteTarget operation: Unsubscribe target before deleting.
```

Anda dapat menggunakan parameter `--force-unsubscribe-all` untuk menghapus target dari semua notifikasi aturan yang dikonfigurasi untuk menggunakannya sebagai target, dan kemudian menghapus target.

```
aws codestar-notifications delete-target --target-address arn:aws:sns:us-east-1:123456789012:MyNotificationTopic --force-unsubscribe-all
```

Konfigurasi integrasi antara notifikasi dan AWS Chatbot

AWS Chatbot adalah AWS layanan yang memungkinkan DevOps dan tim pengembangan perangkat lunak untuk menggunakan ruang obrolan Amazon Chime, saluran Slack, dan saluran Tim Microsoft untuk memantau dan menanggapi peristiwa operasional di AWS Cloud. Anda dapat mengonfigurasi integrasi antara target aturan notifikasi dan AWS Chatbot sehingga pemberitahuan tentang peristiwa muncul di ruang Amazon Chime, saluran Slack, atau saluran Microsoft Teams yang Anda pilih. Untuk informasi selengkapnya, lihat dokumentasi [AWS Chatbot](#).

Sebelum mengonfigurasi integrasi dengan AWS Chatbot, Anda harus mengonfigurasi aturan notifikasi dan target aturan. Untuk informasi selengkapnya, lihat [Pengaturan](#) dan [Membuat aturan](#).

[notifikasi](#). Anda juga harus mengonfigurasi saluran Slack, saluran Microsoft Teams, atau ruang AWS obrolan Amazon Chime di Chatbot. Untuk informasi lebih lanjut, lihat dokumentasi untuk layanan ini.

Topik

- [Konfigurasi klien AWS Chatbot untuk saluran Slack](#)
- [Konfigurasi klien AWS Chatbot untuk saluran Microsoft Teams](#)
- [Konfigurasi klien untuk Slack atau Amazon Chime secara manual](#)

Konfigurasi klien AWS Chatbot untuk saluran Slack

Anda dapat membuat aturan notifikasi yang menggunakan klien AWS Chatbot sebagai target. Jika Anda membuat klien untuk saluran Slack, Anda dapat menggunakan klien ini secara langsung sebagai target dalam alur kerja untuk membuat aturan notifikasi. Ini adalah cara termudah untuk mengatur notifikasi yang muncul di saluran Slack.

Untuk membuat klien AWS Chatbot dengan Slack untuk digunakan sebagai target

1. Ikuti petunjuk dalam [Menyiapkan AWS Chatbot dengan Slack](#) di Panduan Administrator Chatbot AWS . Apabila Anda melakukannya, pertimbangkan pilihan berikut untuk integrasi optimum dengan notifikasi:
 - Saat membuat IAM role, pertimbangkan untuk memilih nama peran yang memudahkan untuk mengidentifikasi tujuan peran ini (misalnya, **AWSCodeStarNotifications-Chatbot-Slack-Role**). Ini dapat membantu Anda mengidentifikasi tujuan peran di masa depan.
 - Dalam topik SNS, Anda tidak harus memilih topik atau AWS Wilayah. Saat Anda memilih klien AWS Chatbot sebagai [target](#), topik Amazon SNS dengan semua izin yang diperlukan dibuat dan dikonfigurasi untuk klien AWS Chatbot sebagai bagian dari proses pembuatan aturan notifikasi.
2. Menyelesaikan proses pembuatan klien. Klien ini kemudian tersedia bagi Anda untuk memilih sebagai target saat membuat aturan notifikasi. Untuk informasi selengkapnya, lihat [Membuat aturan notifikasi](#).

Note

Jangan hapus topik Amazon SNS dari klien Chatbot AWS setelah dikonfigurasi untuk Anda. Melakukan hal tersebut akan mencegah notifikasi dikirim ke Slack.

Konfigurasi klien AWS Chatbot untuk saluran Microsoft Teams

Anda dapat membuat aturan notifikasi yang menggunakan klien AWS Chatbot sebagai target. Jika Anda membuat klien untuk saluran Microsoft Teams, Anda dapat menggunakan klien ini secara langsung sebagai target dalam alur kerja untuk membuat aturan pemberitahuan. Ini adalah cara termudah untuk mengatur notifikasi yang muncul di saluran Microsoft Teams.

Untuk membuat klien AWS Chatbot dengan Microsoft Teams untuk digunakan sebagai target

1. Ikuti petunjuk dalam [Menyiapkan AWS Chatbot dengan Microsoft Teams di Panduan Administrator](#) Chatbot AWS . Apabila Anda melakukannya, pertimbangkan pilihan berikut untuk integrasi optimum dengan notifikasi:
 - Saat membuat IAM role, pertimbangkan untuk memilih nama peran yang memudahkan untuk mengidentifikasi tujuan peran ini (misalnya, **AWSCodeStarNotifications-Chatbot-Microsoft-Teams-Role**). Ini dapat membantu Anda mengidentifikasi tujuan peran di masa depan.
 - Dalam topik SNS, Anda tidak harus memilih topik atau AWS Wilayah. Saat Anda memilih klien AWS Chatbot sebagai [target](#), topik Amazon SNS dengan semua izin yang diperlukan dibuat dan dikonfigurasi untuk klien AWS Chatbot sebagai bagian dari proses pembuatan aturan notifikasi.
2. Menyelesaikan proses pembuatan klien. Klien ini kemudian tersedia bagi Anda untuk memilih sebagai target saat membuat aturan notifikasi. Untuk informasi selengkapnya, lihat [Membuat aturan notifikasi](#).

Note


Jangan hapus topik Amazon SNS dari klien Chatbot AWS setelah dikonfigurasi untuk Anda. Melakukannya akan mencegah pemberitahuan dikirim ke Microsoft Teams.

Konfigurasi klien untuk Slack atau Amazon Chime secara manual

Anda dapat memilih untuk membuat integrasi antara notifikasi dan Slack atau Amazon Chime secara langsung. Ini adalah satu-satunya metode yang tersedia untuk mengonfigurasi notifikasi ke ruang obrolan Amazon Chime. Saat mengonfigurasi integrasi ini secara manual, Anda membuat klien AWS Chatbot yang menggunakan topik Amazon SNS yang sebelumnya telah Anda konfigurasi sebagai target untuk aturan notifikasi.

Untuk mengintegrasikan notifikasi secara manual dengan AWS Chatbot dan slack

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Pilih Pengaturan, lalu pilih Aturan notifikasi.
3. Di Target aturan notifikasi, cari dan salin target.

 Note

Anda dapat mengonfigurasi lebih dari satu aturan notifikasi untuk menggunakan topik Amazon SNS yang sama sebagai target. Ini dapat membantu Anda menggabungkan pesan, tetapi dapat memiliki konsekuensi yang tidak diinginkan jika daftar langganan ditujukan untuk satu aturan atau sumber notifikasi.

4. Buka konsol AWS Chatbot di <https://console.aws.amazon.com/chatbot/>
5. Pilih Konfigurasi klien baru, lalu pilih Slack.
6. Pilih Konfigurasi.
7. Masuk ke ruang kerja Slack Anda.
8. Saat Anda diminta untuk mengonfirmasi pilihan, pilih Izinkan.
9. Pilih Mengonfigurasi saluran baru.
10. Di Detail konfigurasi, di Nama konfigurasi, masukkan nama untuk klien Anda. Ini adalah nama yang akan muncul dalam daftar target yang tersedia untuk jenis target AWS Chatbot (Slack) saat Anda membuat aturan notifikasi.
11. Di Konfigurasi Saluran Slack, di Jenis saluran, pilih Publik atau Privat, tergantung pada jenis saluran yang ingin Anda integrasikan.
 - Di Saluran publik, pilih nama saluran Slack dari daftar.
 - Di ID saluran privat, masukkan kode saluran atau URL.
12. Di Izin IAM, di Peran, pilih Buat IAM role menggunakan templat. Di Templat kebijakan, pilih Izin notifikasi. Di Nama peran, masukkan nama untuk peran ini, (misalnya, **AWSCodeStarNotifications-Chatbot-Slack-Role**). Di Templat kebijakan, pilih Izin notifikasi.
13. Dalam topik SNS, di Wilayah SNS, pilih Wilayah AWS tempat Anda membuat target aturan notifikasi. Di Topik SNS, pilih nama topik Amazon SNS yang dikonfigurasi sebagai target aturan notifikasi.

Note

Langkah ini tidak diperlukan jika Anda akan membuat aturan notifikasi menggunakan klien ini sebagai target.

14. Pilih Konfigurasi.

Note

Jika Anda mengonfigurasi integrasi dengan saluran pribadi, Anda harus mengundang AWS Chatbot ke saluran sebelum Anda akan melihat pemberitahuan di saluran itu. Untuk informasi selengkapnya, lihat dokumentasi [AWS Chatbot](#).

15. (Opsional) Untuk menguji integrasi, buat perubahan dalam sumber daya yang cocok dengan jenis peristiwa untuk aturan notifikasi yang dikonfigurasi untuk menggunakan topik Amazon SNS sebagai target. Misalnya, jika Anda memiliki aturan notifikasi yang dikonfigurasi untuk mengirim notifikasi ketika komentar dibuat pada permintaan tarik, beri komentar pada permintaan tarik dan kemudian tonton saluran Slack di browser untuk melihat kapan notifikasi muncul.

Untuk mengintegrasikan notifikasi dengan AWS Chatbot dan Amazon Chime

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.
2. Pilih Pengaturan, lalu pilih Aturan notifikasi.
3. Di Target aturan notifikasi, cari dan salin target.

Note

Anda dapat mengonfigurasi lebih dari satu aturan notifikasi untuk menggunakan topik Amazon SNS yang sama sebagai target. Ini dapat membantu Anda menggabungkan pesan, tetapi dapat memiliki konsekuensi yang tidak diinginkan jika daftar langganan ditujukan untuk satu aturan atau sumber notifikasi.

4. Di Amazon Chime, buka ruang obrolan yang ingin Anda konfigurasi untuk integrasi.
5. Pilih ikon roda gigi di sudut kanan atas, lalu pilih Kelola kait web.
6. Di kotak dialog Kelola kait web, pilih Baru, masukkan nama untuk kait web, lalu pilih Buat.

7. Verifikasi bahwa kait web muncul, dan kemudian pilih Salin URL kait web.
8. Buka konsol AWS Chatbot di. <https://console.aws.amazon.com/chatbot/>
9. Pilih Konfigurasi klien baru, lalu pilih Amazon Chime.
10. Di Detail konfigurasi, di Nama konfigurasi, masukkan nama untuk klien Anda.
11. Di URL kait web, tempel URL. Di Deskripsi kait web, berikan deskripsi opsional.
12. Di Izin IAM, di Peran, pilih Buat IAM role menggunakan templat. Di Templat kebijakan, pilih Izin notifikasi. Di Nama peran, masukkan nama untuk peran ini, (misalnya, **AWSCodeStarNotifications-Chatbot-Chime-Role**).
13. Dalam topik SNS, di Wilayah SNS, pilih Wilayah AWS tempat Anda membuat target aturan notifikasi. Di Topik SNS, pilih nama topik Amazon SNS yang Anda konfigurasi sebagai target aturan notifikasi.
14. Pilih Konfigurasi.
15. (Opsional) Untuk menguji integrasi, buat perubahan dalam sumber daya yang cocok dengan jenis peristiwa untuk aturan notifikasi yang dikonfigurasi untuk menggunakan topik Amazon SNS sebagai target. Misalnya, jika Anda memiliki aturan notifikasi yang dikonfigurasi untuk mengirim notifikasi saat komentar dibuat atas permintaan tarik, beri komentar pada permintaan tarik, lalu tonton ruang obrolan Amazon Chime untuk melihat kapan notifikasi muncul.

Panggilan API AWS CodeStar Pemberitahuan Pencatatan dengan AWS CloudTrail

AWS CodeStar Notifikasi terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap semua panggilan API untuk notifikasi sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Alat Pengembang dan panggilan kode ke operasi AWS CodeStar Notifications API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk notifikasi. 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 AWS CodeStar Pemberitahuan, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail lainnya.

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

AWS CodeStar Informasi pemberitahuan di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di AWS CodeStar Pemberitahuan, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan riwayat CloudTrail acara](#).

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

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

Semua tindakan AWS CodeStar Pemberitahuan dicatat oleh CloudTrail dan didokumentasikan dalam [AWS CodeStar Notifications API Reference](#). Misalnya, panggilan untuk tindakan `CreateNotificationRule`, `Subscribe`, dan `ListEventTypes` menghasilkan entri di berkas log CloudTrail.

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 gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Memahami entri file log

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

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan pembuatan aturan notifikasi, termasuk Subscribe tindakan CreateNotificationRule dan tindakan.

Note

Beberapa peristiwa dalam entri file log notifikasi mungkin berasal dari peran terkait layanan. `AWSService RoleForCodeStarNotifications`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major"
  },
  "eventTime": "2019-10-07T21:34:41Z",
  "eventSource": "events.amazonaws.com",
  "eventName": "CreateNotificationRule",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "codestar-notifications.amazonaws.com",
  "userAgent": "codestar-notifications.amazonaws.com",
  "requestParameters": {
    "description": "This rule is used to route CodeBuild, CodeCommit, CodePipeline, and other Developer Tools notifications to AWS CodeStar Notifications",
    "name": "awscodestarnotifications-rule",
    "eventPattern": "{\"source\": [\"aws.codebuild\", \"aws.codecommit\", \"aws.codepipeline\"]}"
  },
}
```

```

"responseElements": {
  "ruleArn": "arn:aws:events:us-east-1:123456789012:rule/
awscodestarnotifications-rule"
},
"requestID": "ff1f309a-EXAMPLE",
"eventID": "93c82b07-EXAMPLE",
"eventType": "AwsApiCall",
"apiVersion": "2015-10-07",
"recipientAccountId": "123456789012"
}

```

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major"
  },
  "eventTime": "2019-10-07T21:34:41Z",
  "eventSource": "events.amazonaws.com",
  "eventName": "Subscribe",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "codestar-notifications.amazonaws.com",
  "userAgent": "codestar-notifications.amazonaws.com",
  "requestParameters": {
    "targets": [
      {
        "arn": "arn:aws:codestar-notifications:us-east-1:::",
        "id": "codestar-notifications-events-target"
      }
    ]
  },
  "rule": "awscodestarnotifications-rule"
},
"responseElements": {
  "failedEntryCount": 0,
  "failedEntries": []
},
"requestID": "9466cbda-EXAMPLE",
"eventID": "2f79fdad-EXAMPLE",
"eventType": "AwsApiCall",

```

```
"apiVersion": "2015-10-07",  
"recipientAccountId": "123456789012"  
}
```

Pemecahan Masalah

Informasi berikut dapat membantu Anda memecahkan masalah umum notifikasi.

Topik

- [Saya mendapatkan kesalahan izin saat mencoba membuat aturan notifikasi di sumber daya](#)
- [Saya tidak dapat melihat aturan notifikasi](#)
- [Saya tidak dapat membuat aturan notifikasi](#)
- [Saya menerima notifikasi untuk sumber daya yang tidak dapat saya akses](#)
- [Saya tidak menerima notifikasi Amazon SNS](#)
- [Saya menerima notifikasi duplikat tentang peristiwa](#)
- [Saya ingin memahami mengapa status target notifikasi menunjukkan sebagai tidak terjangkau](#)
- [Saya ingin meningkatkan kuota saya untuk notifikasi dan sumber daya](#)

Saya mendapatkan kesalahan izin saat mencoba membuat aturan notifikasi di sumber daya

Pastikan bahwa Anda memiliki izin yang memadai. Untuk informasi lebih lanjut, lihat [Contoh kebijakan berbasis identitas](#).

Saya tidak dapat melihat aturan notifikasi

Masalah: Saat Anda berada di konsol Alat Developer dan memilih Notifikasi di bawah Pengaturan, Anda melihat kesalahan izin.

Perbaiki yang mungkin: Anda mungkin tidak memiliki izin yang diperlukan untuk melihat notifikasi. Meskipun sebagian besar kebijakan terkelola untuk layanan Alat AWS Pengembang CodePipeline, seperti CodeCommit dan, termasuk izin untuk pemberitahuan, layanan yang saat ini tidak mendukung pemberitahuan tidak menyertakan izin untuk melihatnya. Atau, Anda mungkin memiliki kebijakan khusus yang diterapkan ke pengguna IAM atau peran yang tidak memungkinkan Anda untuk melihat notifikasi. Untuk informasi lebih lanjut, lihat [Contoh kebijakan berbasis identitas](#).

Saya tidak dapat membuat aturan notifikasi

Anda mungkin tidak memiliki izin yang diperlukan untuk membuat aturan notifikasi. Untuk informasi lebih lanjut, lihat [Contoh kebijakan berbasis identitas](#).

Saya menerima notifikasi untuk sumber daya yang tidak dapat saya akses

Ketika Anda membuat aturan notifikasi dan menambahkan target, fitur notifikasi tidak memvalidasi apakah penerima memiliki akses ke sumber daya. Anda dapat menerima notifikasi tentang sumber daya yang tidak dapat diakses. Jika Anda tidak dapat menghapus diri sendiri, minta untuk dihapus dari daftar langganan untuk target.

Saya tidak menerima notifikasi Amazon SNS

Untuk memecahkan masalah dengan topik Amazon SNS, periksa berikut ini:

- Pastikan bahwa topik Amazon SNS dibuat di AWS Wilayah yang sama dengan aturan notifikasi.
- Pastikan alias email Anda berlangganan topik yang benar, dan bahwa Anda telah mengonfirmasi langganan. Untuk informasi selengkapnya, lihat [Berlangganan titik akhir ke topik Amazon SNS](#).
- Verifikasi bahwa kebijakan topik telah diedit untuk memungkinkan AWS CodeStar Pemberitahuan mendorong pemberitahuan ke topik tersebut. Kebijakan topik harus mencakup pernyataan yang serupa dengan yang berikut ini:

```
{
  "Sid": "AWSCodeStarNotifications_publish",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "codestar-notifications.amazonaws.com"
    ]
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopicName",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012"
    }
  }
}
```

Untuk informasi lebih lanjut, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#).

Saya menerima notifikasi duplikat tentang peristiwa

Berikut adalah sebab-sebab yang paling biasa untuk menerima beberapa notifikasi:

- Beberapa notifikasi aturan yang mencakup jenis peristiwa yang sama telah dikonfigurasi untuk sumber daya, dan Anda berlangganan topik Amazon SNS yang target untuk aturan-aturan tersebut. Untuk mengatasi masalah ini, berhenti berlangganan dari salah satu topik atau edit aturan notifikasi untuk menghapus duplikasi.
- Satu atau beberapa target aturan notifikasi terintegrasi dengan AWS Chatbot dan Anda menerima notifikasi di kotak masuk email dan saluran Slack, saluran Microsoft Teams, atau ruang obrolan Amazon Chime. Untuk mengatasi masalah ini, pertimbangkan untuk berhenti berlangganan alamat email Anda dari topik Amazon SNS yang menjadi target aturan dan gunakan saluran Slack, saluran Microsoft Teams, atau ruang obrolan Amazon Chime untuk melihat notifikasi.

Saya ingin memahami mengapa status target notifikasi menunjukkan sebagai tidak terjangkau

Target memiliki kemungkinan dua status: Aktif dan Tidak terjangkau. Tidak terjangkau menunjukkan bahwa notifikasi dikirim ke target, dan pengiriman tidak berhasil. Notifikasi terus dikirim ke target tersebut, dan jika berhasil, status akan diatur ulang ke Aktif.

Target untuk aturan notifikasi mungkin menjadi tidak tersedia untuk salah satu alasan berikut:

- Sumber daya (topik Amazon SNS atau klien Chatbot AWS) telah dihapus. Pilih target lain untuk aturan notifikasi.
- Topik Amazon SNS dienkripsi, dan kebijakan yang diperlukan untuk topik terenkripsi tidak ada, atau kuncinya telah dihapus. AWS KMS Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#).
- Topik Amazon SNS tidak memiliki kebijakan yang diperlukan untuk notifikasi. Notifikasi tidak dapat dikirim ke topik Amazon SNS kecuali memiliki kebijakan. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#).
- Layanan pendukung untuk target (Amazon SNS atau AWS Chatbot) mungkin mengalami masalah.

Saya ingin meningkatkan kuota saya untuk notifikasi dan sumber daya

Saat ini, Anda tidak dapat mengubah kuota apa pun. Lihat [Kuota untuk notifikasi](#).

Kuota untuk notifikasi

Daftar tabel berikut mencantumkan kuota (juga disebut sebagai batas) untuk notifikasi di konsol Alat Developer. Untuk informasi tentang batas yang dapat diubah, lihat [kuota AWS layanan](#).

Sumber Daya	Batas default
Jumlah maksimum aturan notifikasi di AWS akun	1000
Jumlah maksimum target untuk aturan notifikasi	10
Jumlah maksimum aturan notifikasi untuk sumber daya	10

Apa itu koneksi?

Anda dapat menggunakan fitur koneksi di konsol Alat Pengembang untuk menghubungkan AWS sumber daya seperti AWS CodePipeline ke repositori kode eksternal. Fitur ini memiliki API sendiri, [referensi AWS CodeConnections API](#). Setiap koneksi adalah sumber daya yang dapat Anda berikan ke AWS layanan untuk terhubung ke repositori pihak ketiga, seperti Bitbucket. Misalnya, Anda dapat menambahkan koneksi CodePipeline sehingga memicu pipeline Anda saat perubahan kode dilakukan ke repositori kode pihak ketiga Anda. Setiap koneksi diberi nama dan dikaitkan dengan Amazon Resource Name (ARN) unik yang digunakan untuk mereferensikan koneksi tersebut.

Important

Nama layanan AWS CodeStar Connections telah diganti namanya. Sumber daya yang dibuat dengan koneksi codestar namespace sebelumnya akan tetap didukung.

Apa yang bisa saya lakukan dengan koneksi?

Anda dapat menggunakan koneksi untuk mengintegrasikan sumber daya penyedia pihak ketiga dengan sumber AWS daya Anda di alat pengembang, termasuk:

- Connect ke penyedia pihak ketiga, seperti Bitbucket, dan gunakan koneksi pihak ketiga sebagai integrasi sumber dengan sumber AWS daya Anda, seperti CodePipeline.

- Kelola akses ke koneksi Anda secara seragam di seluruh sumber daya Anda dalam CodeBuild membangun proyek, CodeDeploy aplikasi, dan saluran pipa CodePipeline untuk penyedia pihak ketiga Anda.
- Gunakan ARN koneksi di templat tumpukan Anda untuk CodeBuild membangun proyek, CodeDeploy aplikasi, dan saluran pipa CodePipeline, tanpa perlu mereferensikan rahasia atau parameter yang tersimpan.

Untuk penyedia pihak ketiga apa saya dapat membuat koneksi?

Koneksi dapat mengaitkan AWS sumber daya Anda dengan repositori pihak ketiga berikut:

- Azure DevOps
- Bitbucket Cloud
- GitHub.com
- GitHub Awan Perusahaan

Note

Saat ini, domain khusus untuk GitHub Enterprise Cloud tidak didukung.

- GitHub Server Perusahaan
- GitLab.com

Important

Dukungan koneksi untuk GitLab menyertakan versi 15.x dan yang lebih baru.

- GitLab instalasi yang dikelola sendiri (untuk Edisi Perusahaan atau Edisi Komunitas)

Untuk gambaran umum tentang alur kerja koneksi, lihat [Alur kerja untuk membuat atau memperbarui koneksi](#).

Langkah-langkah untuk membuat koneksi untuk jenis penyedia cloud, seperti GitHub, berbeda dari langkah-langkah untuk jenis penyedia yang diinstal, seperti GitHub Enterprise Server. Untuk langkah-langkah tingkat tinggi guna membuat koneksi menurut jenis penyedia, lihat [Bekerja dengan koneksi](#).

Note

Untuk menggunakan koneksi di Eropa (Milan) Wilayah AWS, Anda harus:

1. Instal aplikasi khusus Wilayah
2. Aktifkan Wilayah

Aplikasi khusus Wilayah ini mendukung koneksi di Wilayah Eropa (Milan). Ini diterbitkan di situs penyedia pihak ketiga, dan terpisah dari aplikasi yang ada yang mendukung koneksi untuk Wilayah lain. Dengan menginstal aplikasi ini, Anda memberi wewenang kepada penyedia pihak ketiga untuk membagikan data Anda dengan layanan untuk Wilayah ini saja, dan Anda dapat mencabut izin kapan saja dengan mencopot pemasangan aplikasi.

Layanan tidak akan memproses atau menyimpan data Anda kecuali Anda mengaktifkan Wilayah. Dengan mengaktifkan Wilayah ini, Anda memberikan izin layanan kami untuk memproses dan menyimpan data Anda.

Meskipun Wilayah tidak diaktifkan, penyedia pihak ketiga masih dapat membagikan data Anda dengan layanan kami jika aplikasi khusus Wilayah tetap diinstal, jadi pastikan untuk menghapus instalasi aplikasi setelah Anda menonaktifkan Wilayah. Untuk informasi selengkapnya, lihat [Mengaktifkan Wilayah](#).

Apa yang Layanan AWS terintegrasi dengan koneksi?

Anda dapat menggunakan koneksi untuk mengintegrasikan repositori pihak ketiga Anda dengan yang lain. Layanan AWS Untuk melihat integrasi layanan untuk koneksi, lihat [Integrasi produk dan layanan dengan AWS CodeConnections](#).

Bagaimana koneksi bekerja?

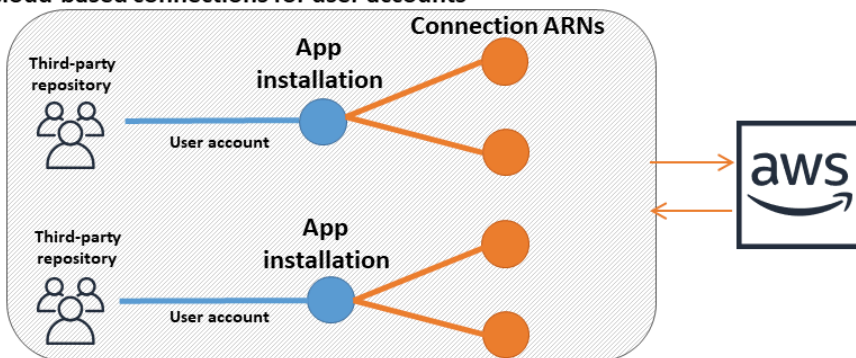
Sebelum Anda dapat membuat koneksi, Anda harus terlebih dahulu menginstal, atau memberikan akses ke, aplikasi AWS otentikasi di akun pihak ketiga Anda. Setelah koneksi diinstal, itu dapat diperbarui untuk menggunakan instalasi ini. Saat Anda membuat koneksi, Anda memberikan akses ke AWS sumber daya di akun pihak ketiga Anda. Ini memungkinkan koneksi untuk mengakses konten, seperti repositori sumber, di akun pihak ketiga, atas nama sumber daya Anda AWS . Anda kemudian dapat berbagi koneksi itu dengan orang lain Layanan AWS untuk menyediakan OAuth koneksi aman antara sumber daya.

Koneksi berbasis cloud dikonfigurasi sebagai berikut dengan perbedaan yang disebut antara akun pengguna atau organisasi.

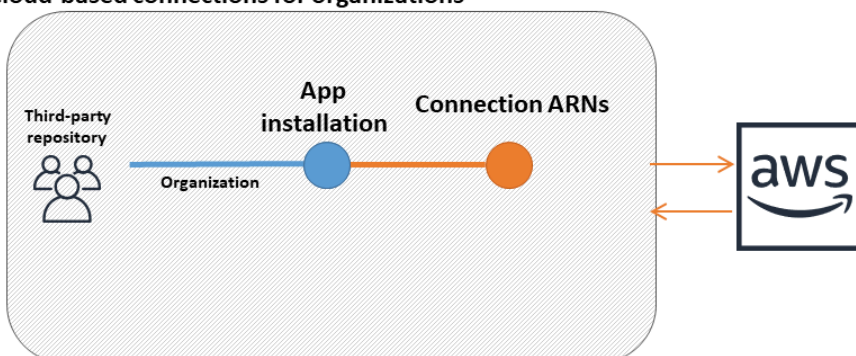
- Akun pengguna: Setiap akun pengguna pihak ketiga berbasis cloud memiliki penginstalan aplikasi konektor. Beberapa koneksi dapat dikaitkan dengan instalasi aplikasi.
- Organizations: Setiap organisasi pihak ketiga berbasis cloud memiliki penginstalan aplikasi konektor. Untuk koneksi dalam organisasi, pemetaan koneksi Anda ke setiap akun Organisasi di organisasi adalah 1:1. Beberapa koneksi tidak dapat dikaitkan dengan instalasi aplikasi. Untuk detail selengkapnya tentang cara organisasi bekerja dengan koneksi, lihat [Bagaimana koneksi dalam AWS CodeConnections bekerja dengan organisasi](#).

Diagram berikut menunjukkan cara kerja koneksi berbasis cloud dengan akun pengguna atau organisasi.

Cloud-based connections for user accounts



Cloud-based connections for organizations



Koneksi dimiliki oleh Akun AWS yang menciptakannya. Koneksi diidentifikasi oleh ARN yang berisi ID koneksi. ID koneksi adalah UUID yang tidak dapat diubah atau dipetakan ulang. Menghapus dan membangun kembali koneksi menghasilkan ID koneksi baru, dan oleh karena itu ARN koneksi baru. Ini berarti koneksi tidak pernah ARNs digunakan kembali.

Koneksi yang baru dibuat berada dalam status Pending. Proses jabat tangan pihak ketiga (OAuth flow) diperlukan untuk menyelesaikan pengaturan koneksi dan untuk berpindah dari Pending ke Available keadaan. Setelah ini selesai, koneksi adalah Available dan dapat digunakan dengan AWS layanan, seperti CodePipeline.

Jika Anda ingin membuat sambungan ke jenis penyedia yang diinstal (on-prem), seperti Server GitHub Perusahaan atau GitLab dikelola sendiri, Anda menggunakan sumber daya host dengan koneksi Anda.

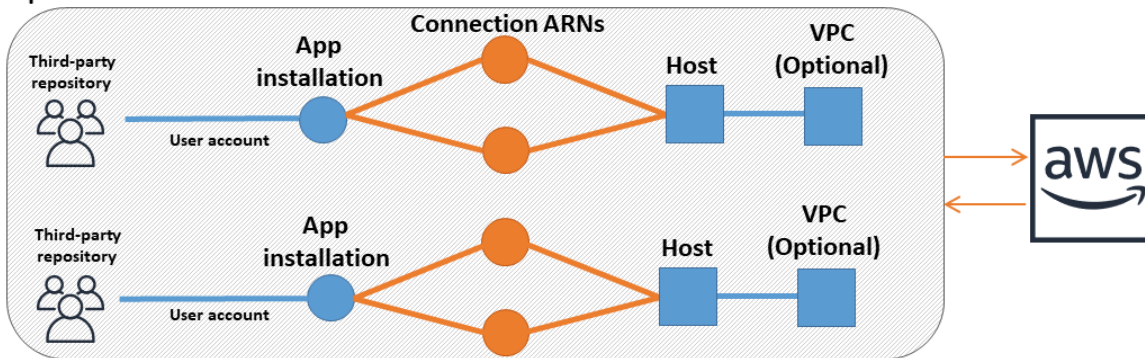
Koneksi on-prem dikonfigurasi sebagai berikut dengan perbedaan yang disebut antara akun pengguna atau organisasi.

- Akun pengguna: Setiap akun pengguna pihak ketiga di prem memiliki instalasi aplikasi konektor. Beberapa koneksi untuk penyedia on-prem dapat dikaitkan dengan satu host.
- Organizations: Setiap organisasi pihak ketiga di prem memiliki instalasi aplikasi konektor. Untuk koneksi lokal di organisasi, seperti GitHub Organizations for GitHub Enterprise Server, Anda membuat host baru untuk setiap koneksi di organisasi Anda dan pastikan untuk memasukkan informasi yang sama di bidang jaringan (VPC, Subnet IDs, dan Grup IDs Keamanan) untuk host. Untuk detail selengkapnya tentang cara organisasi bekerja dengan koneksi, lihat [Bagaimana koneksi dalam AWS CodeConnections bekerja dengan organisasi](#).
- Semua: Untuk setiap koneksi on-prem, setiap VPC hanya dapat dikaitkan dengan satu host pada satu waktu.

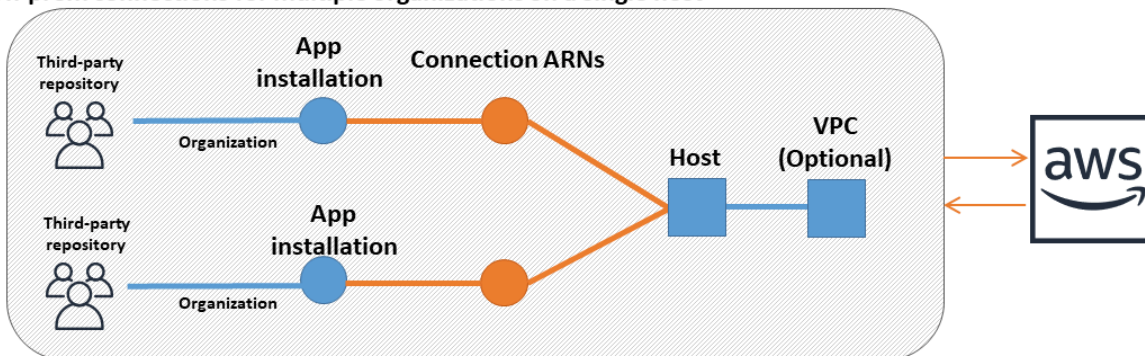
Dalam semua kasus, Anda harus memberikan URL untuk server on-prem Anda. Selain itu, jika server berada dalam VPC pribadi (yaitu, tidak dapat diakses melalui internet), Anda harus memberikan informasi VPC bersama dengan informasi sertifikat TLS opsional. Konfigurasi ini memungkinkan CodeConnections untuk berkomunikasi dengan instance dan dibagikan oleh semua koneksi yang dibuat untuk host ini. Misalnya, untuk satu instance GitHub Enterprise Server, Anda akan membuat satu aplikasi yang diwakili oleh Host. Kemudian, untuk konfigurasi akun pengguna, Anda dapat membuat beberapa koneksi untuk host tersebut, yang sesuai dengan penginstalan aplikasi Anda seperti yang ditunjukkan pada diagram berikut. Jika tidak, untuk organisasi, Anda membuat satu instalasi aplikasi dan koneksi untuk host tersebut.

Diagram berikut menunjukkan bagaimana koneksi on-prem bekerja dengan akun pengguna atau organisasi.

On-prem connections for user accounts



On-prem connections for multiple organizations on a single host



Host yang baru dibuat berada dalam status Pending. Proses pendaftaran pihak ketiga diperlukan untuk menyelesaikan penyiapan host dan untuk berpindah dari status Pending ke Available. Setelah ini selesai, host Available dan dapat digunakan untuk koneksi ke jenis penyedia yang diinstal.

Untuk gambaran umum tentang alur kerja koneksi, lihat [Alur kerja untuk membuat atau memperbarui koneksi](#). Untuk ikhtisar alur kerja pembuatan host untuk penyedia yang diinstal, lihat [Alur kerja untuk membuat atau memperbarui host](#). Untuk langkah-langkah tingkat tinggi guna membuat koneksi menurut jenis penyedia, lihat [Bekerja dengan koneksi](#).

Bagaimana koneksi dalam AWS CodeConnections bekerja dengan organisasi

Untuk organisasi dengan penyedia, seperti GitHub Organizations, Anda tidak dapat menginstal GitHub aplikasi ke beberapa GitHub Organizations. Koneksi memiliki pemetaan 1:1 dengan organisasi melalui penggunaan aplikasi konektor Github. Aplikasi konektor harus terpisah untuk setiap organisasi di GitHub atau Server GitHub Perusahaan dan harus memiliki koneksi yang terkait dengannya.

Misalnya, untuk bekerja dengan beberapa organisasi di GitHub server yang sama, Anda harus membuat koneksi terpisah untuk setiap organisasi dan menginstal GitHub aplikasi terpisah untuk organisasi ini. Akun target di sisi Github, bagaimanapun, bisa sama.

Alur kerja untuk membuat atau memperbarui koneksi

Saat membuat koneksi, Anda juga membuat atau menggunakan instalasi aplikasi konektor yang ada untuk jabat tangan autentikasi dengan penyedia pihak ketiga.

Koneksi dapat memiliki status berikut:

- **Pending** - Koneksi pending adalah koneksi yang harus diselesaikan (dipindahkan ke `available`) sebelum dapat digunakan.
- **Available** - Anda dapat menggunakan atau meneruskan koneksi `available` ke sumber daya dan pengguna lain di akun Anda.
- **Error** - Koneksi yang memiliki status `error` akan dicoba ulang secara otomatis. Itu tidak dapat digunakan sampai `available`.

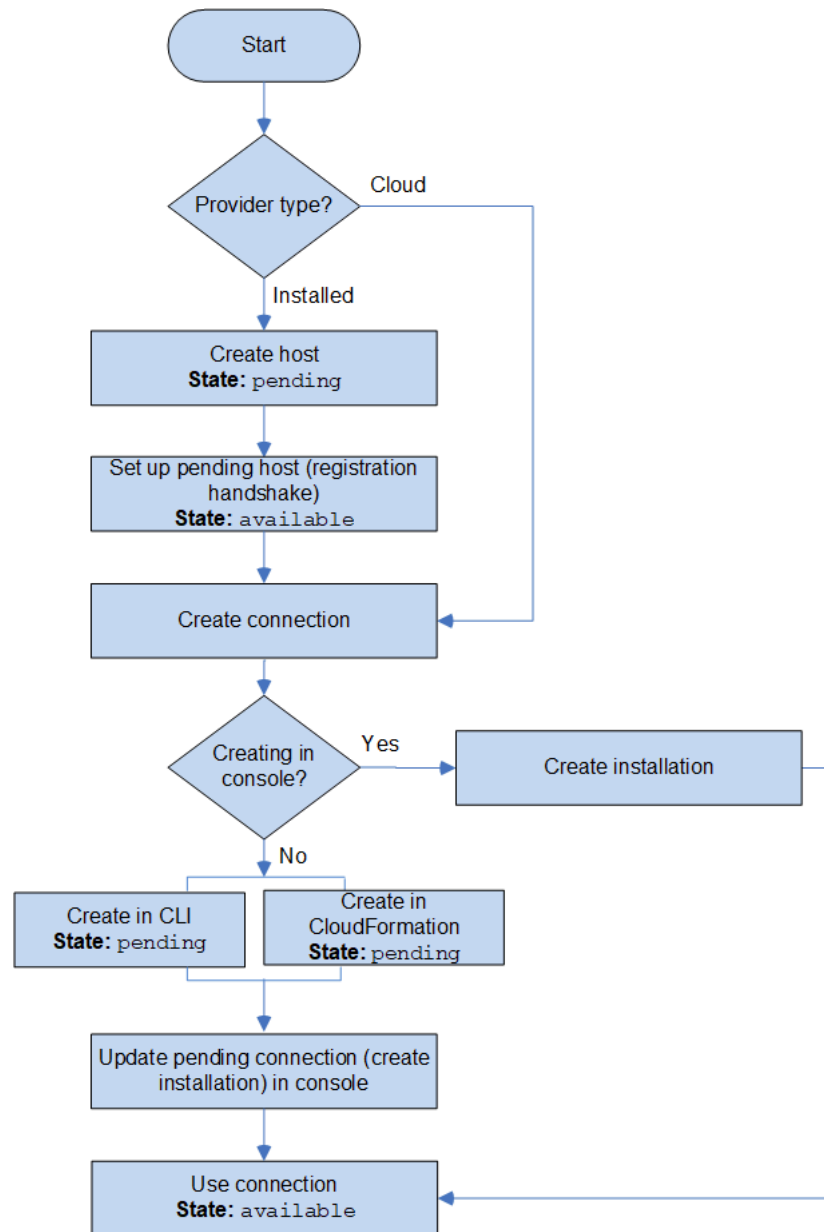
Alur Kerja: Membuat atau memperbarui koneksi dengan CLI, SDK, atau AWS CloudFormation

Anda menggunakan [CreateConnection](#) API untuk membuat koneksi menggunakan AWS Command Line Interface (AWS CLI), SDK, atau CloudFormation. Setelah dibuat, koneksi berada dalam status `pending`. Anda menyelesaikan proses dengan menggunakan opsi konsol Siapkan koneksi yang tertunda. Konsol meminta Anda untuk membuat instalasi atau menggunakan instalasi yang sudah ada untuk koneksi. Anda kemudian menggunakan konsol untuk menyelesaikan jabat tangan dan memindahkan koneksi ke status `available` dengan memilih Selesaikan koneksi di konsol.

Alur kerja: Membuat atau memperbarui koneksi dengan konsol

Jika Anda membuat koneksi ke jenis penyedia yang diinstal, seperti GitHub Enterprise Server, Anda terlebih dahulu membuat host. Jika Anda terhubung ke jenis penyedia cloud, seperti Bitbucket, Anda melewatkan pembuatan host dan melanjutkan membuat koneksi.

Untuk membuat atau memperbarui koneksi menggunakan konsol, Anda menggunakan halaman tindakan CodePipeline edit di konsol untuk memilih penyedia pihak ketiga Anda. Konsol meminta Anda untuk membuat instalasi atau menggunakan instalasi yang sudah ada untuk koneksi, dan kemudian menggunakan konsol untuk membuat koneksi. Konsol menyelesaikan jabat tangan dan memindahkan koneksi dari status `pending` ke `available` secara otomatis.



Alur kerja untuk membuat atau memperbarui host

Saat Anda membuat koneksi untuk penyedia yang diinstal (on-prem), Anda menggunakan sumber daya host.

Note

Untuk organisasi di Server GitHub Perusahaan atau yang GitLab dikelola sendiri, Anda tidak melewati host yang tersedia. Anda membuat host baru untuk setiap koneksi di organisasi Anda, dan Anda harus memastikan untuk memasukkan informasi yang sama di bidang jaringan (ID VPC, Subnet IDs, dan Grup Keamanan IDs) untuk host. Untuk informasi

selengkapnya, lihat [Koneksi dan penyiapan host untuk penyedia terinstal yang mendukung organisasi](#).

Host dapat memiliki status berikut:

- **Pending**- pending Host adalah host yang telah dibuat dan harus diatur (dipindahkan ke `available`) sebelum dapat digunakan.
- **Available**- Anda dapat menggunakan atau meneruskan `available` host ke koneksi Anda.

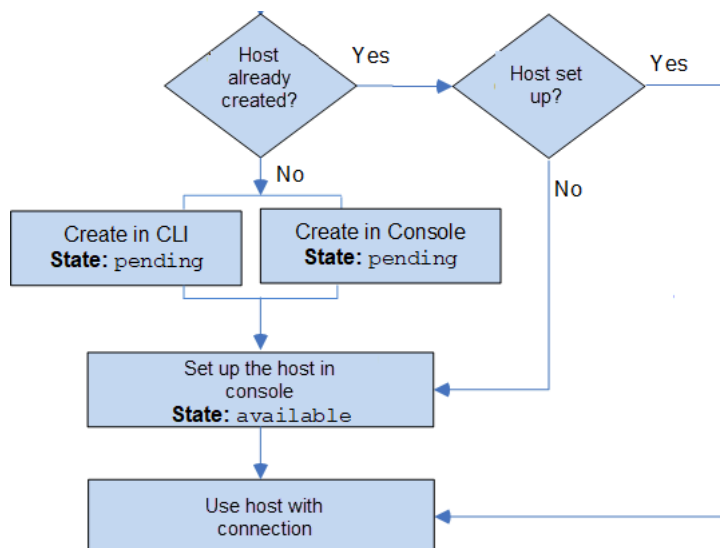
Alur Kerja: Membuat atau memperbarui host dengan CLI, SDK, atau AWS CloudFormation

Anda menggunakan [CreateHost](#) API untuk membuat host menggunakan AWS Command Line Interface (AWS CLI), SDK, atau CloudFormation. Setelah dibuat, tuan rumah dalam pending keadaan. Anda menyelesaikan proses dengan menggunakan opsi Pengaturan konsol di konsol.

Alur kerja: Membuat atau memperbarui host dengan konsol

Jika Anda membuat sambungan ke jenis penyedia yang diinstal, seperti Server GitHub Perusahaan atau GitLab dikelola sendiri, Anda membuat host atau menggunakan host yang ada. Jika Anda terhubung ke jenis penyedia cloud, seperti Bitbucket, Anda melewati pembuatan host dan melanjutkan membuat koneksi.

Gunakan konsol untuk mengatur host dan mengubah statusnya dari pending ke `available`.



Sumber daya global di AWS CodeConnections

Koneksi adalah sumber daya global, yang berarti bahwa sumber daya direplikasi di semua Wilayah AWS.

Meskipun format ARN koneksi mencerminkan nama Wilayah tempatnya dibuat, sumber daya tidak dibatasi ke Wilayah mana pun. Wilayah tempat sumber daya koneksi dibuat adalah Wilayah tempat pembaruan data sumber daya koneksi dikendalikan. Contoh operasi API yang mengendalikan pembaruan ke data sumber daya koneksi termasuk membuat koneksi, memperbarui penginstalan, menghapus koneksi, atau menandai koneksi.

Sumber daya host untuk koneksi bukanlah sumber daya yang tersedia secara global. Anda menggunakan sumber daya host hanya di Wilayah tempat mereka dibuat.

- Anda hanya perlu membuat koneksi sekali, dan kemudian Anda dapat menggunakannya di mana saja Wilayah AWS.
- Jika Wilayah tempat koneksi dibuat mengalami masalah, hal ini berdampak pada data sumber daya koneksi APIs yang mengontrol, tetapi Anda masih dapat berhasil menggunakan koneksi di setiap Wilayah lainnya.
- Ketika Anda mencantumkan sumber daya koneksi di konsol atau CLI, daftar tersebut menampilkan semua sumber daya koneksi yang terkait dengan akun Anda di semua Wilayah.
- Ketika Anda mencantumkan sumber daya host di konsol atau CLI, daftar tersebut menampilkan sumber daya host yang terkait dengan akun Anda hanya di Wilayah yang dipilih.
- Ketika koneksi dengan sumber daya host terkait terdaftar atau dilihat dengan CLI, output mengembalikan ARN host terlepas dari Wilayah CLI yang dikonfigurasi.

Bagaimana saya memulai dengan koneksi?

Untuk memulai, berikut adalah beberapa topik yang berguna untuk ditinjau:

- Mempelajari tentang [konsep](#) untuk koneksi.
- Menyiapkan [sumber daya yang Anda butuhkan](#) untuk mulai bekerja dengan koneksi.
- Memulai dengan [koneksi pertama](#) Anda dan menghubungkannya ke sumber daya.

Konsep koneksi

Menyiapkan dan menggunakan fitur koneksi lebih mudah jika Anda memahami konsep dan istilahnya. Berikut adalah beberapa konsep yang perlu diketahui saat Anda menggunakan koneksi di konsol Alat Developer:

instalasi

Contoh AWS aplikasi di akun pihak ketiga. Menginstal aplikasi AWS CodeStar Konektor memungkinkan AWS untuk mengakses sumber daya dalam akun pihak ketiga. Instalasi hanya dapat diedit di situs web penyedia pihak ketiga.

koneksi

AWS Sumber daya yang digunakan untuk menghubungkan repositori sumber pihak ketiga ke layanan lain AWS .

repositori pihak ketiga

Repositori yang disediakan oleh layanan atau perusahaan yang bukan bagian dari AWS. Misalnya, repositori Bitbucket adalah repositori pihak ketiga.

jenis penyedia

Layanan atau perusahaan yang menyediakan repositori sumber pihak ketiga yang ingin Anda hubungkan. Anda menghubungkan AWS sumber daya Anda ke jenis penyedia eksternal. Jenis penyedia tempat repositori sumber diinstal pada jaringan dan infrastruktur adalah jenis penyedia yang diinstal. Misalnya, GitHub Enterprise Server adalah jenis penyedia yang diinstal.

host

Sumber daya yang mewakili infrastruktur tempat penyedia pihak ketiga diinstal. Koneksi menggunakan host untuk mewakili server tempat penyedia pihak ketiga Anda diinstal, seperti GitHub Enterprise Server. Anda membuat satu host untuk semua koneksi ke jenis penyedia tersebut.

Note

Saat Anda menggunakan konsol untuk membuat koneksi ke GitHub Enterprise Server, konsol akan membuat sumber daya host untuk Anda sebagai bagian dari proses.

AWS CodeConnections penyedia dan versi yang didukung

Bab ini memberikan informasi tentang penyedia dan versi yang AWS CodeConnections mendukung.

Topik

- [Jenis penyedia yang didukung untuk Azure DevOps](#)
- [Jenis penyedia yang didukung untuk Bitbucket](#)
- [Jenis penyedia yang didukung untuk GitHub dan GitHub Enterprise Cloud](#)
- [Jenis dan versi penyedia yang didukung untuk GitHub Enterprise Server](#)
- [Jenis penyedia yang didukung untuk GitLab.com](#)
- [Jenis penyedia yang didukung untuk dikelola GitLab sendiri](#)

Jenis penyedia yang didukung untuk Azure DevOps

Anda dapat menggunakan aplikasi koneksi dengan Azure DevOps.

Jenis penyedia yang diinstal (dihosting), seperti Azure Cloud Hosting, tidak didukung.

Jenis penyedia yang didukung untuk Bitbucket

Anda dapat menggunakan aplikasi koneksi dengan Atlassian Bitbucket Cloud.

Jenis penyedia Bitbucket yang diinstal, seperti Bitbucket Server, tidak didukung.

Jenis penyedia yang didukung untuk GitHub dan GitHub Enterprise Cloud

Anda dapat menggunakan aplikasi koneksi dengan GitHub dan GitHub Enterprise Cloud.

Important

AWS CodeConnections belum mendukung GitHub Enterprise Cloud dengan residensi data (domain*.ghe.com kustom).

Jenis dan versi penyedia yang didukung untuk GitHub Enterprise Server

Anda dapat menggunakan aplikasi koneksi dengan versi GitHub Enterprise Server yang didukung.

Untuk daftar versi yang didukung, lihat <https://enterprise.github.com/releases/>.

⚠ Important

AWS CodeConnections tidak mendukung versi GitHub Enterprise Server yang tidak digunakan lagi. Misalnya, AWS CodeConnections tidak mendukung GitHub Enterprise Server versi 2.22.0 karena masalah yang diketahui dalam rilis. Untuk menghubungkan, tingkatkan ke versi 2.22.1 atau versi terbaru yang tersedia.

Jenis penyedia yang didukung untuk GitLab.com

Anda dapat menggunakan koneksi dengan GitLab.com. Untuk informasi selengkapnya, lihat [Buat koneksi ke GitLab](#).

⚠ Important

Dukungan koneksi untuk GitLab menyertakan versi 15.x dan yang lebih baru.

Jenis penyedia yang didukung untuk dikelola GitLab sendiri

Anda dapat menggunakan koneksi dengan instalasi yang GitLab dikelola sendiri (untuk Edisi Perusahaan atau Edisi Komunitas). Lihat informasi yang lebih lengkap di [Buat koneksi ke GitLab self-managed](#).

Integrasi produk dan layanan dengan AWS CodeConnections

AWS CodeConnections terintegrasi dengan sejumlah AWS layanan dan produk dan layanan mitra. Gunakan informasi di bagian berikut untuk membantu Anda mengonfigurasi koneksi agar terintegrasi dengan produk dan layanan yang Anda gunakan.

Sumber daya terkait berikut dapat membantu Anda ketika bekerja dengan layanan ini.

Topik

- [CodeGuru Peninjau Amazon](#)
- [Amazon Q Developer](#)
- [Amazon SageMaker](#)
- [AWS App Runner](#)
- [AWS CloudFormation](#)

- [AWS CodeBuild](#)
- [AWS CodePipeline](#)
- [Service Catalog](#)
- [AWS Proton](#)

CodeGuru Peninjau Amazon

[CodeGuru Reviewer](#) adalah layanan untuk memantau kode repositori Anda. Anda dapat menggunakan koneksi untuk mengaitkan repositori pihak ketiga yang memiliki kode yang ingin Anda tinjau. Untuk tutorial di mana Anda mempelajari cara mengonfigurasi CodeGuru Reviewer untuk memantau kode sumber dalam GitHub repositori sehingga dapat membuat rekomendasi yang meningkatkan kode, lihat [Tutorial: memantau kode sumber dalam GitHub repositori di Panduan Pengguna Amazon CodeGuru Reviewer](#).

Amazon Q Developer

Amazon Q Developer adalah asisten percakapan bertenaga AI generatif yang dapat membantu Anda memahami, membangun, memperluas, dan mengoperasikan aplikasi. AWS Untuk informasi selengkapnya, lihat [Apa itu Pengembang Amazon Q?](#) di Panduan Pengguna Pengembang Amazon Q.

Amazon SageMaker

[Amazon SageMaker](#) adalah layanan untuk membangun, melatih, dan menerapkan model bahasa pembelajaran mesin. Untuk tutorial di mana Anda mengonfigurasi koneksi ke GitHub repositori, lihat [Panduan SageMaker MLOps Proyek Menggunakan Repos Git Pihak Ketiga di Panduan Pengembang Amazon SageMaker](#).

AWS App Runner

[AWS App Runner](#) adalah layanan yang menyediakan cara yang cepat, sederhana, dan hemat biaya untuk menyebarkan dari kode sumber atau gambar kontainer langsung ke aplikasi web yang dapat diskalakan dan aman di. AWS Cloud Anda dapat menerapkan kode aplikasi dari repositori Anda dengan integrasi otomatis App Runner dan pipeline pengiriman. Anda dapat menggunakan koneksi untuk menyebarkan kode sumber Anda ke layanan App Runner dari repositori pribadi GitHub . Untuk informasi selengkapnya, lihat [Penyedia repositori kode sumber](#) di Panduan AWS App Runner Pengembang.

AWS CloudFormation

[AWS CloudFormation](#) adalah layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya Anda sehingga Anda dapat menghabiskan lebih sedikit waktu mengelola sumber daya tersebut dan lebih banyak waktu untuk berfokus pada aplikasi Anda yang berjalan AWS. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti instans Amazon EC2 atau instans Amazon RDS DB), dan CloudFormation menangani penyediaan dan konfigurasi sumber daya tersebut untuk Anda.

Anda menggunakan koneksi dengan sinkronisasi Git CloudFormation untuk membuat konfigurasi sinkronisasi yang memantau repositori Git Anda. Untuk tutorial yang memandu Anda menggunakan sinkronisasi Git untuk penerapan tumpukan, lihat [Bekerja dengan sinkronisasi CloudFormation Git](#) di CloudFormation Panduan Pengguna.

Untuk informasi selengkapnya CloudFormation, lihat [Mendaftarkan akun Anda untuk mempublikasikan CloudFormation ekstensi](#) di Panduan Pengguna Antarmuka Baris CloudFormation Perintah.

AWS CodeBuild

[AWS CodeBuild](#) adalah layanan untuk membangun dan menguji kode Anda. CodeBuild menghilangkan kebutuhan untuk menyediakan, mengelola, dan menskalakan server build Anda sendiri, dan menyediakan lingkungan build yang dikemas untuk bahasa pemrograman populer dan alat build. Untuk informasi selengkapnya tentang penggunaan CodeBuild dengan koneksi ke GitLab, lihat [GitLabkoneksi](#) di Panduan AWS CodeBuild Pengguna.

AWS CodePipeline

[CodePipeline](#) adalah layanan pengiriman berkelanjutan yang dapat Anda gunakan untuk memodelkan, memvisualisasikan, dan mengotomatiskan langkah-langkah yang diperlukan untuk merilis perangkat lunak Anda. Anda dapat menggunakan koneksi untuk mengonfigurasi repositori pihak ketiga untuk tindakan CodePipeline sumber.

Pelajari lebih lanjut:

- Lihat halaman referensi konfigurasi CodePipeline tindakan untuk `SourceConnections` tindakan. Untuk melihat parameter konfigurasi dan JSON/YAML cuplikan contoh, lihat [CodeStarSourceConnection](#) di AWS CodePipeline Panduan Pengguna.
- Untuk melihat tutorial Memulai yang membuat pipeline dengan repositori sumber pihak ketiga, lihat [Memulai dengan koneksi](#)

Service Catalog

[Service Catalog](#) memungkinkan organisasi untuk membuat dan mengelola katalog produk yang disetujui untuk digunakan. AWS

Ketika Anda mengotorisasi koneksi antara penyedia repositori eksternal Anda Akun AWS , seperti, GitHub Enterprise, atau Bitbucket GitHub, koneksi memungkinkan Anda untuk menyinkronkan produk Service Catalog ke file template yang dikelola melalui repositori pihak ketiga.

Untuk informasi selengkapnya, lihat [Menyinkronkan produk Service Catalog ke file template dari GitHub, GitHub Enterprise, atau Bitbucket](#) di Panduan Pengguna Service Catalog.

AWS Proton

[AWS Proton](#) adalah layanan berbasis cloud untuk menyebarkan ke infrastruktur cloud. Anda dapat menggunakan koneksi untuk membuat tautan ke repositori pihak ketiga Anda untuk sumber daya di templat Anda. AWS Proton Untuk informasi selengkapnya, lihat [Membuat tautan ke repositori Anda](#) di AWS Proton Panduan Pengguna.

Menyiapkan koneksi

Selesaikan tugas dalam bagian ini untuk menyiapkan pembuatan dan penggunaan fitur koneksi di konsol Alat Developer.

Topik

- [Mendaftar untuk Akun AWS](#)
- [Membuat dan menerapkan kebijakan dengan izin untuk membuat koneksi](#)

Mendaftar untuk Akun AWS

Untuk memulai AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat [Memulai dengan Akun AWS](#) di Panduan AWS Account Management Referensi.

Membuat dan menerapkan kebijakan dengan izin untuk membuat koneksi

Cara menggunakan editor kebijakan JSON untuk membuat kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.

2. Pada panel navigasi di sebelah kiri, pilih Kebijakan.

Jika ini pertama kalinya Anda memilih Kebijakan, akan muncul halaman Selamat Datang di Kebijakan Terkelola. Pilih Memulai.

3. Di bagian atas halaman, pilih Buat kebijakan.
4. Di bagian Editor kebijakan, pilih opsi JSON.
5. Masukkan dokumen kebijakan JSON berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateConnection",
        "codeconnections>DeleteConnection",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:GetInstallationUrl",
        "codeconnections:GetIndividualAccessToken",
        "codeconnections:ListInstallationTargets",
        "codeconnections:StartOAuthHandshake",
        "codeconnections:UpdateConnectionInstallation",
        "codeconnections:UseConnection"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

6. Pilih Berikutnya.

Note

Anda dapat beralih antara opsi editor Visual dan JSON kapan saja. Namun, jika Anda melakukan perubahan atau memilih Berikutnya di editor Visual, IAM dapat merestrukturisasi kebijakan Anda untuk mengoptimalkannya bagi editor visual. Untuk informasi selengkapnya, lihat [Restrukturisasi kebijakan](#) dalam Panduan Pengguna IAM.

7. Pada halaman Tinjau dan buat, masukkan Nama kebijakan dan Deskripsi (opsional) untuk kebijakan yang Anda buat. Tinjau Izin yang ditentukan dalam kebijakan ini untuk melihat izin yang diberikan oleh kebijakan Anda.
8. Pilih Buat kebijakan untuk menyimpan kebijakan baru Anda.

Memulai dengan koneksi

Cara termudah untuk memulai koneksi adalah dengan mengatur koneksi yang mengaitkan repositori sumber pihak ketiga Anda ke sumber daya Anda. AWS Jika Anda ingin menghubungkan pipeline Anda ke AWS sumber, seperti CodeCommit, Anda akan menghubungkannya sebagai tindakan sumber. Namun, jika Anda memiliki repositori eksternal, Anda harus membuat koneksi untuk mengaitkan repositori Anda dengan alur Anda. Dalam tutorial ini, Anda mengatur koneksi dengan repositori Bitbucket dan alur Anda.

Di bagian ini, Anda menggunakan koneksi dengan:

- AWS CodePipeline: Dalam langkah-langkah ini, Anda membuat alur dengan repositori Bitbucket Anda sebagai sumber alur.
- [Amazon CodeGuru Reviewer](#): Selanjutnya, Anda mengaitkan repositori Bitbucket Anda ke umpan balik dan alat analisis Anda di Reviewer. CodeGuru

Topik

- [Prasyarat](#)
- [Langkah 1: Edit file sumber Anda](#)
- [Langkah 2: Buat alur Anda](#)
- [Langkah 3: Kaitkan repositori Anda dengan Reviewer CodeGuru](#)

Prasyarat

Sebelum memulai, selesaikan langkah-langkah di [Pengaturan](#). Anda juga memerlukan repositori sumber pihak ketiga yang ingin Anda sambungkan ke AWS layanan Anda dan memungkinkan koneksi untuk mengelola otentikasi untuk Anda. Misalnya, Anda mungkin ingin menghubungkan repositori Bitbucket ke AWS layanan Anda yang terintegrasi dengan repositori sumber.

- Buat repositori Bitbucket dengan akun Bitbucket Anda.

- Siapkan kredensial Bitbucket Anda. Ketika Anda menggunakan Konsol Manajemen AWS untuk mengatur koneksi, Anda diminta untuk masuk dengan kredensial Bitbucket Anda.

Langkah 1: Edit file sumber Anda

Saat Anda membuat repositori Bitbucket, file README .md default disertakan, yang akan Anda edit.

1. Masuk ke repositori Bitbucket Anda dan pilih Sumber.
2. Pilih file README .md dan pilih Edit di bagian atas halaman. Hapus teks yang ada dan tambahkan teks berikut.

```
This is a Bitbucket repository!
```

3. Pilih Lakukan.

Pastikan file README .md berada di tingkat root repositori Anda..

Langkah 2: Buat alur Anda

Dalam bagian ini, Anda membuat alur dengan tindakan berikut:

- Tahap sumber dengan koneksi ke repositori dan tindakan Bitbucket Anda.
- Tahap build dengan aksi AWS CodeBuild build.


Untuk membuat alur dengan wizard

1. Masuk ke CodePipeline konsol di <https://console.aws.amazon.com/codepipeline/>.
2. Pada halaman Selamat Datang, halaman Memulai, atau halaman Alur, pilih Buat alur.
3. Di Langkah 1: Pilih pengaturan alur, di Nama alur, masukkan **MyBitbucketPipeline**.
4. Di Peran layanan, pilih Peran layanan baru.

Note

Jika Anda memilih untuk menggunakan peran CodePipeline layanan yang ada, pastikan Anda telah menambahkan izin `codeconnections:UseConnection` IAM ke kebijakan peran layanan Anda. Untuk petunjuk tentang peran CodePipeline layanan, lihat [Menambahkan izin ke peran CodePipeline layanan](#).

5. Di bawah Pengaturan lanjutan, biarkan default. Di Penyimpanan artifact, pilih Lokasi default untuk menggunakan penyimpanan artifact default, seperti bucket artifact Amazon S3 yang ditetapkan sebagai default, untuk alur Anda di Wilayah yang Anda pilih untuk alur Anda.

 Note

Ini bukan bucket sumber untuk kode sumber Anda. Ini adalah penyimpanan artifact untuk alur Anda. Penyimpanan artifact terpisah, seperti bucket S3, diperlukan untuk setiap alur.

Pilih Selanjutnya.

6. Pada halaman Langkah 2: Tambahkan tahap sumber, tambahkan tahap sumber:
 - a. Di Penyedia sumber, pilih Bitbucket.
 - b. Pada Koneksi, pilih Hubungkan ke Bitbucket.
 - c. Pada halaman Hubungkan ke Bitbucket, di Nama koneksi, masukkan nama untuk koneksi yang ingin Anda buat. Nama membantu Anda mengidentifikasi koneksi ini nanti.

Pada Aplikasi Bitbucket, pilih Instal aplikasi baru.

- d. Pada halaman instalasi aplikasi, sebuah pesan menunjukkan bahwa AWS CodeStar aplikasi sedang mencoba untuk terhubung ke akun Bitbucket Anda. Pilih Berikan akses. Setelah Anda mengotorisasi koneksi, repositori Anda di Bitbucket terdeteksi, dan Anda dapat memilih untuk mengaitkannya dengan sumber daya Anda. AWS
- e. ID koneksi untuk instalasi baru Anda ditampilkan. Pilih Selesaikan koneksi. Anda akan dikembalikan ke CodePipeline konsol.
- f. Di Nama repositori, pilih nama repositori Bitbucket Anda.
- g. Dalam nama Branch, pilih cabang untuk repositori Anda.
- h. Pastikan opsi Mulai pipeline pada perubahan kode sumber dipilih.
- i. Di bawah Format artefak keluaran, pilih salah satu dari berikut ini: CodePipeline default.
 - Pilih CodePipeline default untuk menggunakan format zip default untuk artefak di pipeline.
 - Pilih klon lengkap untuk menyertakan metadata Git tentang repositori artefak dalam pipeline. Ini hanya didukung untuk CodeBuild tindakan.

Pilih Berikutnya.

7. Di Tambahkan tahap membangun, tambahkan sebuah tahap membangun:
 - a. Di Penyedia pembangunan, pilih AWS CodeBuild. Izinkan Wilayah ke default ke Wilayah alur.
 - b. Pilih Buat proyek.
 - c. Di Nama proyek, masukkan nama untuk proyek pembangunan ini.
 - d. Di Citra lingkungan, pilih Citra terkelola. Untuk Sistem operasi, pilih Ubuntu.
 - e. Untuk Waktu aktif, pilih Standar. Untuk Gambar, pilih:5.0aws/codebuild/standard.
 - f. Untuk Peran layanan, pilih Peran layanan baru.
 - g. Pada Buildspec, untuk Spesifikasi membangun, pilih Sisipkan perintah membangun. Pilih Beralih ke editor, dan tempel berikut ini di Perintah membangun:

```
version: 0.2

phases:
  install:
    #If you use the Ubuntu standard image 2.0 or later, you must specify
    runtime-versions.
    #If you specify runtime-versions and use an image other than Ubuntu
    standard image 2.0, the build fails.
    runtime-versions:
      nodejs: 12
      # name: version
    #commands:
      # - command
      # - command
  pre_build:
    commands:
      - ls -lt
      - cat README.md
  # build:
    #commands:
      # - command
      # - command
  #post_build:
    #commands:
      # - command
      # - command
#artifacts:
#files:
```

```
# - location
# - location
#name: $(date +%Y-%m-%d)
#discard-paths: yes
#base-directory: location
#cache:
#paths:
# - paths
```

- h. Pilih Lanjutkan ke CodePipeline. Ini kembali ke CodePipeline konsol dan membuat CodeBuild proyek yang menggunakan perintah build Anda untuk konfigurasi. Proyek build menggunakan peran layanan untuk mengelola izin AWS layanan. Langkah ini mungkin memakan waktu beberapa menit.
 - i. Pilih Selanjutnya.
8. Pada halaman Langkah 4: Tambahkan tahap men-deploy, pilih Lewati tahap men-deploy, dan kemudian terima pesan peringatan dengan memilih Lewati lagi. Pilih Selanjutnya.
 9. Pada Langkah 5: Tinjauan, pilih Buat alur.
 10. Ketika alur Anda berhasil dibuat, eksekusi alur dimulai.

The screenshot displays two stages of a pipeline execution. The top stage is 'Source', which has succeeded. Below it is a 'Disable transition' button. The bottom stage is 'Build', which has also succeeded. Both stages show a 'Source: README.md edited online with Bitbucket' message.

11. Pada tahap membangun Anda yang berhasil, pilih Detail.

Di bawah Detail eksekusi, lihat keluaran CodeBuild build. Perintah mengeluarkan isi file README.md sebagai berikut:

```
This is a Bitbucket repository!
```

```
35 [Container] 2020/06/05 19:14:51 Running command cat README.md
36 This is a Bitbucket repository!
37 [Container] 2020/06/05 19:14:51 Phase complete: PRE_BUILD State: SUCCEEDED
38 [Container] 2020/06/05 19:14:51 Phase context status code: Message:
39 [Container] 2020/06/05 19:14:51 Entering phase BUILD
40 [Container] 2020/06/05 19:14:51 Phase complete: BUILD State: SUCCEEDED
41 [Container] 2020/06/05 19:14:51 Phase context status code: Message:
42 [Container] 2020/06/05 19:14:51 Entering phase POST_BUILD
43 [Container] 2020/06/05 19:14:51 Phase complete: POST_BUILD State: SUCCEEDED
44 [Container] 2020/06/05 19:14:51 Phase context status code: Message:
```

Langkah 3: Kaitkan repositori Anda dengan Reviewer CodeGuru

Setelah Anda membuat koneksi, Anda dapat menggunakan koneksi itu untuk semua sumber AWS daya Anda di akun yang sama. Misalnya, Anda dapat menggunakan koneksi Bitbucket yang sama untuk tindakan CodePipeline sumber dalam pipeline dan analisis komit repositori Anda di Reviewer CodeGuru

1. Masuk ke konsol CodeGuru Reviewer.
2. Di bawah CodeGuru Reviewer, pilih Repositori asosiasi.

Wizard satu halaman terbuka.

3. Pada Pilih penyedia sumber, pilih Bitbucket.
4. Di bawah Connect to Bitbucket (with AWS CodeConnections), pilih koneksi yang Anda buat untuk pipeline.
5. Pada Lokasi repositori, pilih nama repositori Bitbucket Anda, lalu pilih Kaitkan.

Anda dapat melanjutkan untuk mengatur tinjauan kode. Untuk informasi selengkapnya, lihat [Menghubungkan ke Bitbucket untuk mengaitkan repositori dengan CodeGuru Reviewer di Panduan Pengguna](#) Amazon CodeGuru Reviewer.

Bekerja dengan koneksi

Koneksi adalah konfigurasi yang Anda gunakan untuk menghubungkan AWS sumber daya ke repositori kode eksternal. Setiap koneksi adalah sumber daya yang dapat diberikan ke layanan seperti untuk terhubung AWS CodePipeline ke repositori pihak ketiga seperti Bitbucket. Misalnya, Anda dapat menambahkan koneksi CodePipeline sehingga memicu pipeline Anda saat perubahan kode dilakukan ke repositori kode pihak ketiga Anda. Anda juga dapat menghubungkan AWS sumber daya Anda ke jenis penyedia yang diinstal seperti GitHub Enterprise Server.

Note

Untuk organisasi di GitHub atau Server GitHub Perusahaan, Anda tidak dapat menginstal GitHub Aplikasi ke beberapa GitHub Organizations. Aplikasi untuk pemetaan GitHub Organisasi adalah pemetaan 1:1. Satu organisasi hanya dapat memiliki satu aplikasi pada satu waktu; Namun, Anda dapat memiliki beberapa koneksi yang menunjuk ke aplikasi yang sama. Untuk detail selengkapnya, lihat [Bagaimana koneksi dalam AWS CodeConnections bekerja dengan organisasi](#).

Jika Anda ingin membuat koneksi ke jenis penyedia yang diinstal, seperti GitHub Enterprise Server, konsol akan membuat host untuk Anda. Host adalah sumber daya yang Anda buat untuk mewakili server tempat penyedia Anda diinstal. Untuk informasi selengkapnya, lihat [Bekerja dengan host](#).

Saat membuat koneksi, Anda menggunakan wizard di konsol untuk menginstal aplikasi koneksi dengan penyedia pihak ketiga Anda dan mengaitkannya dengan koneksi baru. Jika Anda sudah menginstal aplikasi, Anda dapat menggunakannya.

Note

Untuk menggunakan koneksi di Eropa (Milan) Wilayah AWS, Anda harus:

1. Instal aplikasi khusus Wilayah
2. Aktifkan Wilayah

Aplikasi khusus Wilayah ini mendukung koneksi di Wilayah Eropa (Milan). Ini diterbitkan di situs penyedia pihak ketiga, dan terpisah dari aplikasi yang ada yang mendukung koneksi untuk Wilayah lain. Dengan menginstal aplikasi ini, Anda memberi wewenang kepada penyedia pihak ketiga untuk membagikan data Anda dengan layanan untuk Wilayah ini saja, dan Anda dapat mencabut izin kapan saja dengan mencopot pemasangan aplikasi. Layanan tidak akan memproses atau menyimpan data Anda kecuali Anda mengaktifkan Wilayah. Dengan mengaktifkan Wilayah ini, Anda memberikan izin layanan kami untuk memproses dan menyimpan data Anda.

Meskipun Wilayah tidak diaktifkan, penyedia pihak ketiga masih dapat membagikan data Anda dengan layanan kami jika aplikasi khusus Wilayah tetap diinstal, jadi pastikan untuk menghapus instalasi aplikasi setelah Anda menonaktifkan Wilayah. Untuk informasi selengkapnya, lihat [Mengaktifkan Wilayah](#).

Untuk informasi selengkapnya tentang koneksi, lihat [referensi AWS CodeConnections API](#).

Untuk informasi selengkapnya tentang tindakan CodePipeline sumber untuk Bitbucket, lihat [CodestarConnectionSource](#) di Panduan AWS CodePipeline Pengguna.

Untuk membuat atau melampirkan kebijakan ke pengguna AWS Identity and Access Management (IAM) atau peran Anda dengan izin yang diperlukan untuk menggunakan koneksi, lihat [AWS CodeConnections referensi izin](#) Bergantung pada kapan peran CodePipeline layanan Anda dibuat, Anda mungkin perlu memperbarui izinnya untuk mendukung AWS CodeConnections. Untuk instruksi, lihat [Perbarui peran layanan](#) di Panduan Pengguna AWS CodePipeline .

Topik

- [Buat koneksi](#)
- [Buat koneksi ke Azure DevOps](#)
- [Membuat koneksi ke Bitbucket](#)
- [Buat koneksi ke GitHub](#)
- [Membuat koneksi ke GitHub Enterprise Server](#)
- [Buat koneksi ke GitLab](#)
- [Buat koneksi ke GitLab self-managed](#)
- [Memperbarui koneksi yang tertunda](#)
- [Daftar koneksi](#)
- [Menghapus koneksi](#)
- [Menandai sumber daya koneksi](#)
- [Melihat detail koneksi](#)
- [Berbagi koneksi dengan Akun AWS](#)

Buat koneksi

Anda dapat membuat koneksi ke jenis penyedia pihak ketiga berikut:

- Untuk membuat koneksi ke Bitbucket, lihat [Membuat koneksi ke Bitbucket](#).
- Untuk membuat sambungan ke GitHub atau GitHub Enterprise Cloud, lihat [Buat koneksi ke GitHub](#).
- Untuk membuat sambungan ke Server GitHub Perusahaan, termasuk membuat sumber daya host Anda, lihat [Membuat koneksi ke GitHub Enterprise Server](#).
- Untuk membuat koneksi ke GitLab, lihat [Buat koneksi ke GitLab](#).
- Untuk membuat sambungan ke Azure DevOps, lihat [Membuat koneksi ke DevOps Azure](#).

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan codeconnections ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Buat koneksi ke Azure DevOps

Anda dapat menggunakan Konsol Manajemen AWS or the AWS Command Line Interface (AWS CLI) untuk membuat koneksi ke repositori yang dihosting di Azure. DevOps

Sebelum Anda memulai:

- Anda harus sudah membuat akun dengan Azure DevOps.
- Anda harus sudah membuat proyek dan repositori Azure di portal Azure. DevOps Akun Anda harus memiliki akses administrator ke repositori.

Note

Anda dapat membuat koneksi ke DevOps repositori Azure. Jenis penyedia Azure yang diinstal (pada host), seperti Azure Cloud Hosting, tidak didukung. Lihat [AWS CodeConnections penyedia dan versi yang didukung](#).

Note

Koneksi hanya menyediakan akses ke repositori yang dimiliki oleh akun yang digunakan untuk membuat koneksi.

Topik

- [Buat koneksi ke Azure DevOps \(konsol\)](#)
- [Buat koneksi ke Azure DevOps \(CLI\)](#)

Buat koneksi ke Azure DevOps (konsol)

Anda dapat menggunakan konsol untuk membuat koneksi ke Azure DevOps.

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan codeconnections ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Langkah 1: Buat koneksi Anda

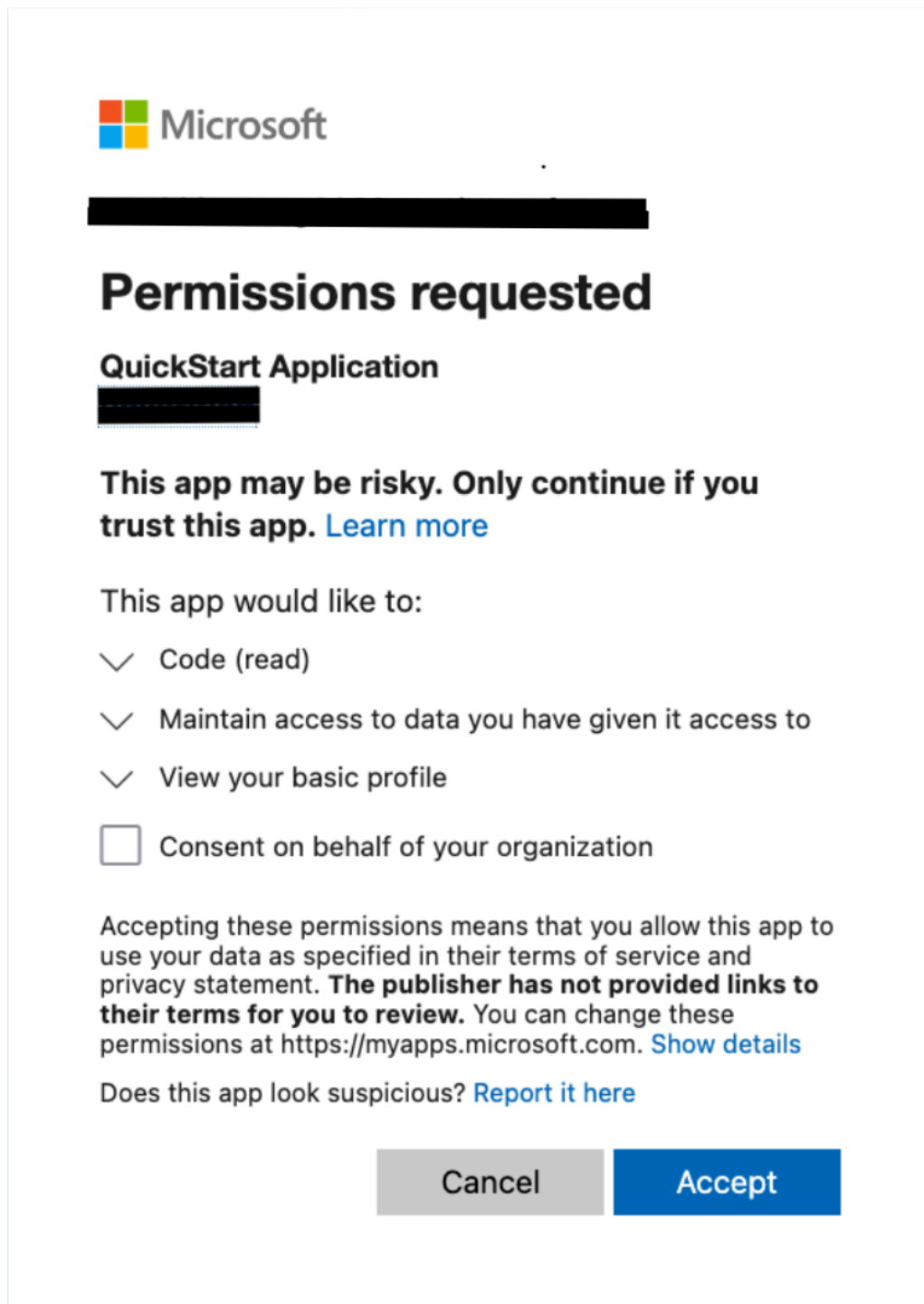
1. Masuk ke Konsol Manajemen AWS, dan buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan > Koneksi, lalu pilih Buat koneksi.
3. Untuk membuat sambungan ke DevOps repositori Azure, di bawah Pilih penyedia, pilih Azure. DevOps Di Nama koneksi, masukkan nama untuk koneksi yang ingin Anda buat. Pilih Connect to Azure DevOps, dan lanjutkan ke Langkah 2.

The screenshot shows the 'Create a connection' page in the AWS CodeSuite settings. The page has a title 'Create a connection' with an 'Info' link and a '+' icon. Under the heading 'Select a provider', there are six radio button options: Bitbucket, GitHub, GitHub Enterprise Server, GitLab, GitLab self-managed, and Azure DevOps. The 'Azure DevOps' option is selected. Below this is a section titled 'Create Azure DevOps connection' with an 'Info' link. It contains a 'Connection name' input field. At the bottom right, there is an orange button labeled 'Connect to Azure DevOps'. There is also a section for 'Tags - optional' which is currently collapsed.

Langkah 2: Connect ke Azure DevOps

1. Pada halaman DevOps Pengaturan Connect to Azure, nama koneksi Anda akan ditampilkan.
2. Jika halaman login untuk Microsoft ditampilkan, masuk dengan kredensial Anda dan kemudian pilih untuk melanjutkan.

Anda mungkin perlu memberikan izin jika ini adalah pertama kalinya Anda membuat koneksi ke Azure DevOps dari Konsol Manajemen AWS



3. Pilih Terima.
4. Pada halaman koneksi, ID koneksi untuk instalasi baru Anda ditampilkan.
5. Pilih Connect untuk membuat koneksi. Koneksi yang dibuat ditampilkan dalam daftar koneksi dan sekarang dalam status yang tersedia dan siap digunakan.

Buat koneksi ke Azure DevOps (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk membuat koneksi.

Untuk melakukannya, gunakan perintah `create-connection`.

Important

Koneksi yang dibuat melalui AWS CLI atau AWS CloudFormation dalam PENDING status secara default. Setelah Anda membuat koneksi dengan CLI atau CloudFormation, gunakan konsol untuk mengedit koneksi untuk membuat statusnya. AVAILABLE

Untuk membuat koneksi ke Azure DevOps

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-connection` perintah, menentukan `--provider-type` dan `--connection-name` untuk koneksi Anda. Dalam contoh ini, nama penyedia pihak ketiga adalah `AzureDevOps` dan nama koneksi yang ditentukan adalah `MyConnection`.

```
aws codeconnections create-connection --provider-type AzureDevOps --connection-name MyConnection
```

Jika berhasil, perintah ini mengembalikan informasi ARN koneksi seperti berikut ini.

```
{
  "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
}
```

2. Gunakan konsol untuk menyelesaikan koneksi. Untuk informasi selengkapnya, lihat [Memperbarui koneksi yang tertunda](#).

Membuat koneksi ke Bitbucket

Anda dapat menggunakan Konsol Manajemen AWS or the AWS Command Line Interface (AWS CLI) untuk membuat koneksi ke repositori yang dihosting di bitbucket.org.

Sebelum Anda memulai:

- Anda harus sudah membuat akun dengan Bitbucket.
- Anda harus sudah membuat repositori kode di bitbucket.org.

Note

Anda dapat membuat koneksi ke repositori Bitbucket Cloud. Jenis penyedia Bitbucket yang diinstal, seperti Bitbucket Server, tidak didukung. Lihat [AWS CodeConnections penyedia dan versi yang didukung](#).

Note

Koneksi hanya menyediakan akses ke repositori yang dimiliki oleh akun yang digunakan untuk membuat koneksi.

Jika aplikasi sedang diinstal di ruang kerja Bitbucket, Anda perlu Mengelola izin ruang kerja. Jika tidak, opsi untuk menginstal aplikasi tidak akan ditampilkan.

Topik

- [Membuat koneksi ke Bitbucket \(konsol\)](#)
- [Membuat koneksi ke Bitbucket \(CLI\)](#)

Membuat koneksi ke Bitbucket (konsol)

Anda dapat menggunakan konsol untuk membuat koneksi ke Bitbucket.

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan `codeconnections` ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Langkah 1: Buat koneksi Anda

1. Masuk ke Konsol Manajemen AWS, dan buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan > Koneksi, lalu pilih Buat koneksi.

3. Untuk membuat koneksi ke repositori Bitbucket, pada Pilih penyedia layanan, pilih Bitbucket. Di Nama koneksi, masukkan nama untuk koneksi yang ingin Anda buat. Pilih Hubungkan ke Bitbucket, dan lanjutkan ke Langkah 2.

Developer Tools > Connections > Create connection

Create a connection [Info](#)

Select a provider

Bitbucket GitHub GitHub Enterprise Server

Create Bitbucket connection

Connection name

[Connect to Bitbucket](#)

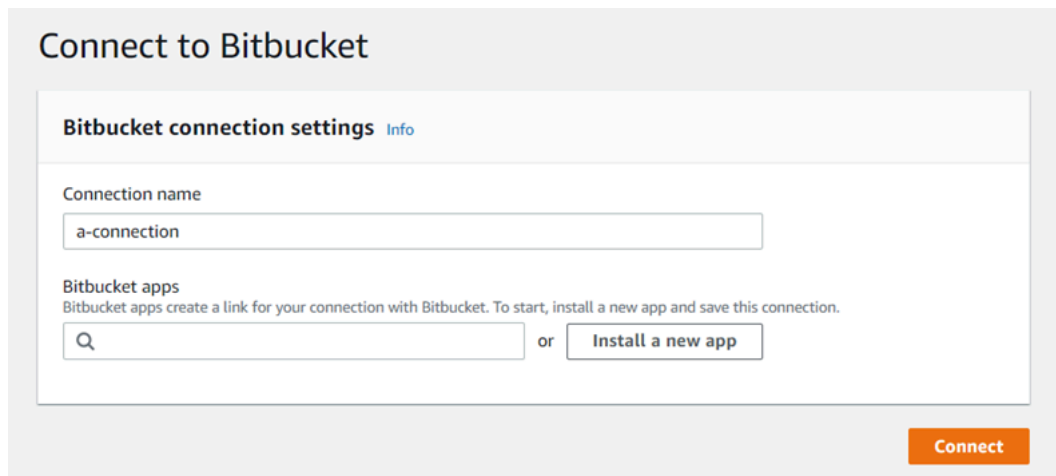
Langkah 2: Hubungkan ke Bitbucket

1. Pada halaman pengaturan Hubungkan ke Bitbucket, nama koneksi Anda ditampilkan.

Pada Aplikasi Bitbucket, pilih penginstalan aplikasi atau pilih Instal aplikasi baru untuk membuatnya.

Note

Anda hanya menginstal aplikasi sekali untuk setiap ruang kerja atau akun Bitbucket. Jika Anda telah menginstal aplikasi Bitbucket, pilih aplikasi tersebut dan lanjutkan ke langkah terakhir di bagian ini.



Connect to Bitbucket

Bitbucket connection settings [Info](#)

Connection name

a-connection

Bitbucket apps
Bitbucket apps create a link for your connection with Bitbucket. To start, install a new app and save this connection.

or

2. Jika halaman masuk untuk Bitbucket ditampilkan, masuk dengan kredensial Anda lalu pilih untuk melanjutkan.
3. Pada halaman instalasi aplikasi, sebuah pesan menunjukkan bahwa AWS CodeStar aplikasi sedang mencoba untuk terhubung ke akun Bitbucket Anda.

Jika Anda menggunakan ruang kerja Bitbucket, ubah opsi Otorisasi untuk ke ruang kerja. Hanya ruang kerja di mana Anda memiliki akses administrator yang akan ditampilkan.

Pilih Berikan akses.



AWS CodeStar requests access

This app is hosted at <https://codestar-connections.webhooks.aws>

Read your account information

Read your repositories and their pull requests

Administer your repositories

Read and modify your repositories

Authorize for

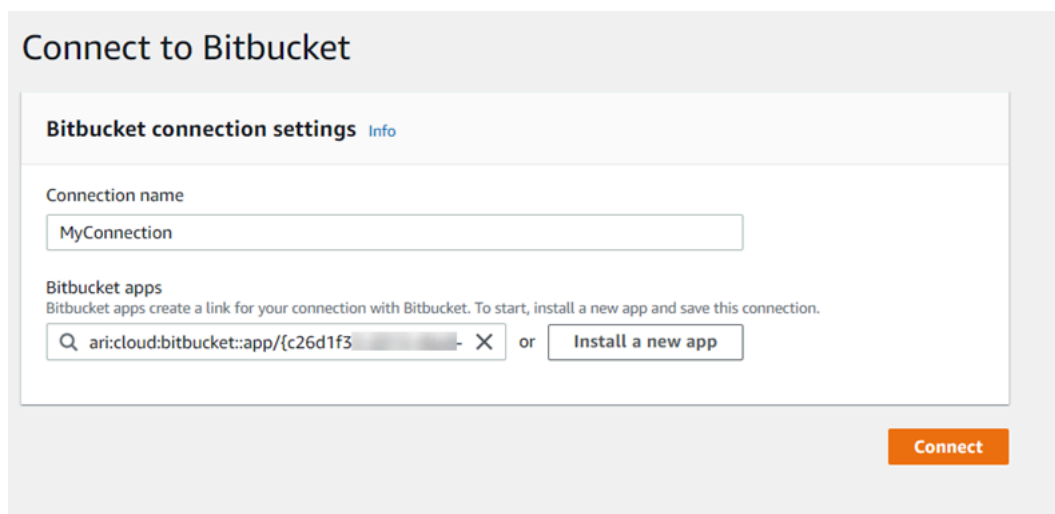
Allow AWS CodeStar to do this?

This 3rd party vendor has not provided a privacy policy or terms of use.

Atlassian's Privacy Policy is not applicable to the use of this App.

[Grant access](#) [Cancel](#)

4. Di Aplikasi Bitbucket, ID koneksi untuk instalasi baru Anda ditampilkan. Pilih Hubungkan. Koneksi yang dibuat ditampilkan dalam daftar koneksi.



Membuat koneksi ke Bitbucket (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk membuat koneksi.

Untuk melakukannya, gunakan perintah `create-connection`.

Important

Koneksi yang dibuat melalui AWS CLI atau AWS CloudFormation dalam PENDING status secara default. Setelah Anda membuat koneksi dengan CLI atau CloudFormation, gunakan konsol untuk mengedit koneksi untuk membuat statusnya. AVAILABLE

Untuk membuat koneksi ke Bitbucket

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-connection` perintah, menentukan `--provider-type` dan `--connection-name` untuk koneksi Anda. Dalam contoh ini, nama penyedia pihak ketiga adalah Bitbucket dan nama koneksi yang ditentukan adalah MyConnection.

```
aws codeconnections create-connection --provider-type Bitbucket --connection-name
MyConnection
```

Jika berhasil, perintah ini mengembalikan informasi ARN koneksi seperti berikut ini.

```
{
  "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
}
```

2. Gunakan konsol untuk menyelesaikan koneksi. Untuk informasi selengkapnya, lihat [Memperbarui koneksi yang tertunda](#).

Buat koneksi ke GitHub

Anda dapat menggunakan Konsol Manajemen AWS atau AWS Command Line Interface (AWS CLI) untuk membuat koneksi ke GitHub.

Sebelum Anda memulai:

- Anda harus sudah membuat akun dengan GitHub.
- Anda harus sudah membuat repositori kode pihak ketiga Anda.

Note

Untuk membuat koneksi, Anda harus menjadi pemilik GitHub organisasi. Untuk repositori yang tidak berada di bawah organisasi, Anda harus menjadi pemilik repositori.

Topik

- [Buat koneksi ke GitHub \(konsol\)](#)
- [Buat koneksi ke GitHub \(CLI\)](#)

Buat koneksi ke GitHub (konsol)

Anda dapat menggunakan konsol untuk membuat koneksi ke GitHub.

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan `codeconnections` ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

1. Masuk ke Konsol Manajemen AWS, dan buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan > Koneksi, lalu pilih Buat koneksi.
3. Untuk membuat sambungan ke GitHub atau repositori GitHub Enterprise Cloud, di bawah Pilih penyedia, pilih. GitHub Di Nama koneksi, masukkan nama untuk koneksi yang ingin Anda buat. Pilih Connect to GitHub, dan lanjutkan ke Langkah 2.

[Developer Tools](#) > [Connections](#) > Create connection

Create a connection Info

Select a provider

Bitbucket

GitHub

GitHub Enterprise Server

GitLab

GitLab self-managed

Create GitHub App connection Info

Connection name

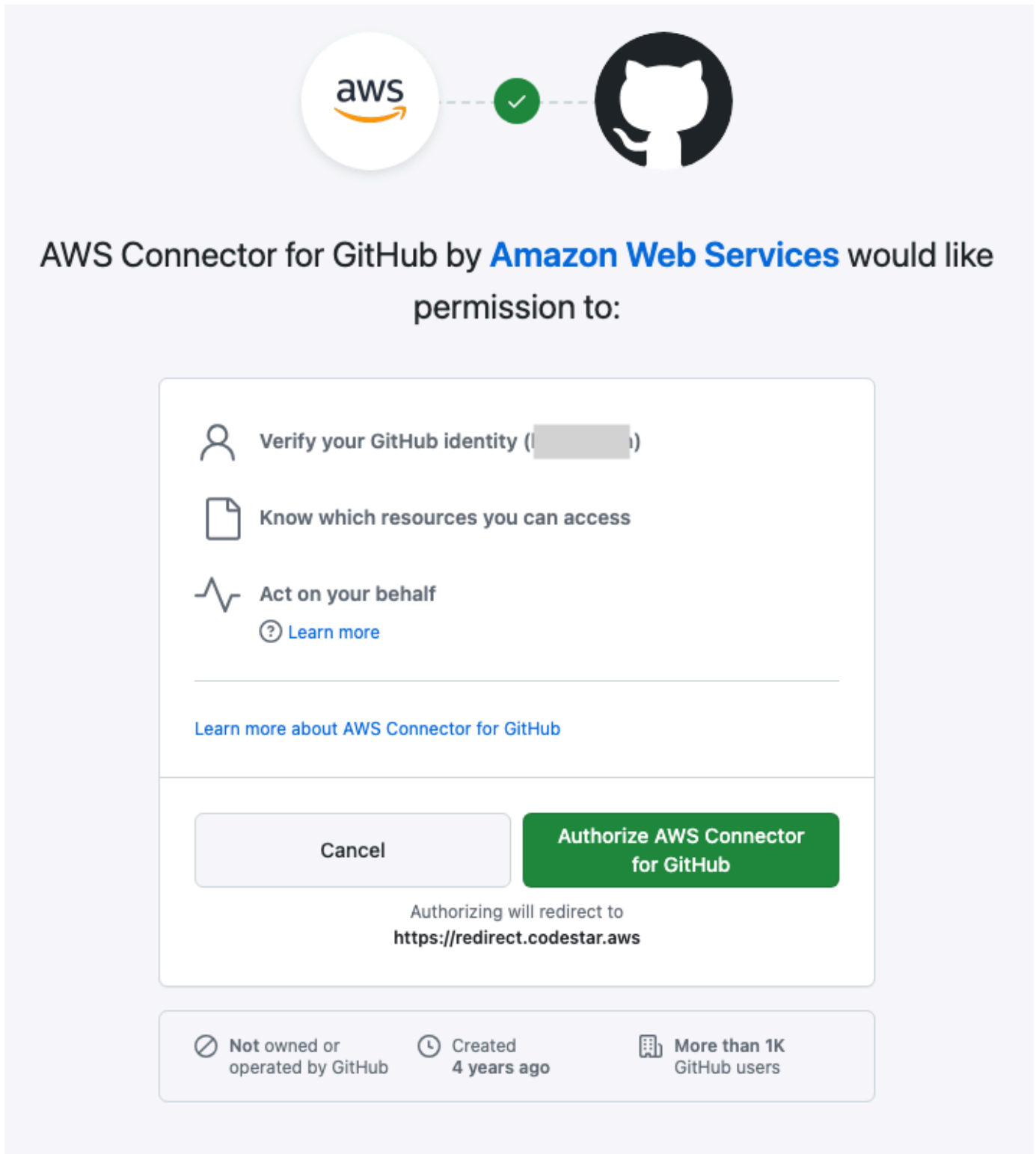
github-connection

► **Tags - optional**

[Connect to GitHub](#)

Untuk membuat koneksi ke GitHub

1. Di bawah pengaturan GitHub koneksi, nama koneksi Anda muncul di Nama koneksi. Pilih [Connect to GitHub](#). Halaman permintaan akses muncul.



2. Pilih Otorisasi AWS Konektor untuk GitHub. Halaman koneksi menampilkan dan menampilkan bidang GitHub Aplikasi.

Connect to GitHub

GitHub connection settings [Info](#)


Connection name

App installation - optional
Install GitHub App to connect as a bot. Alternatively, leave it blank to connect as a GitHub user, which can be used in AWS CodeBuild projects.

 or

► **Tags - optional**

- Di bawah GitHub Aplikasi, pilih penginstalan aplikasi atau pilih Instal aplikasi baru untuk membuatnya.

 Note

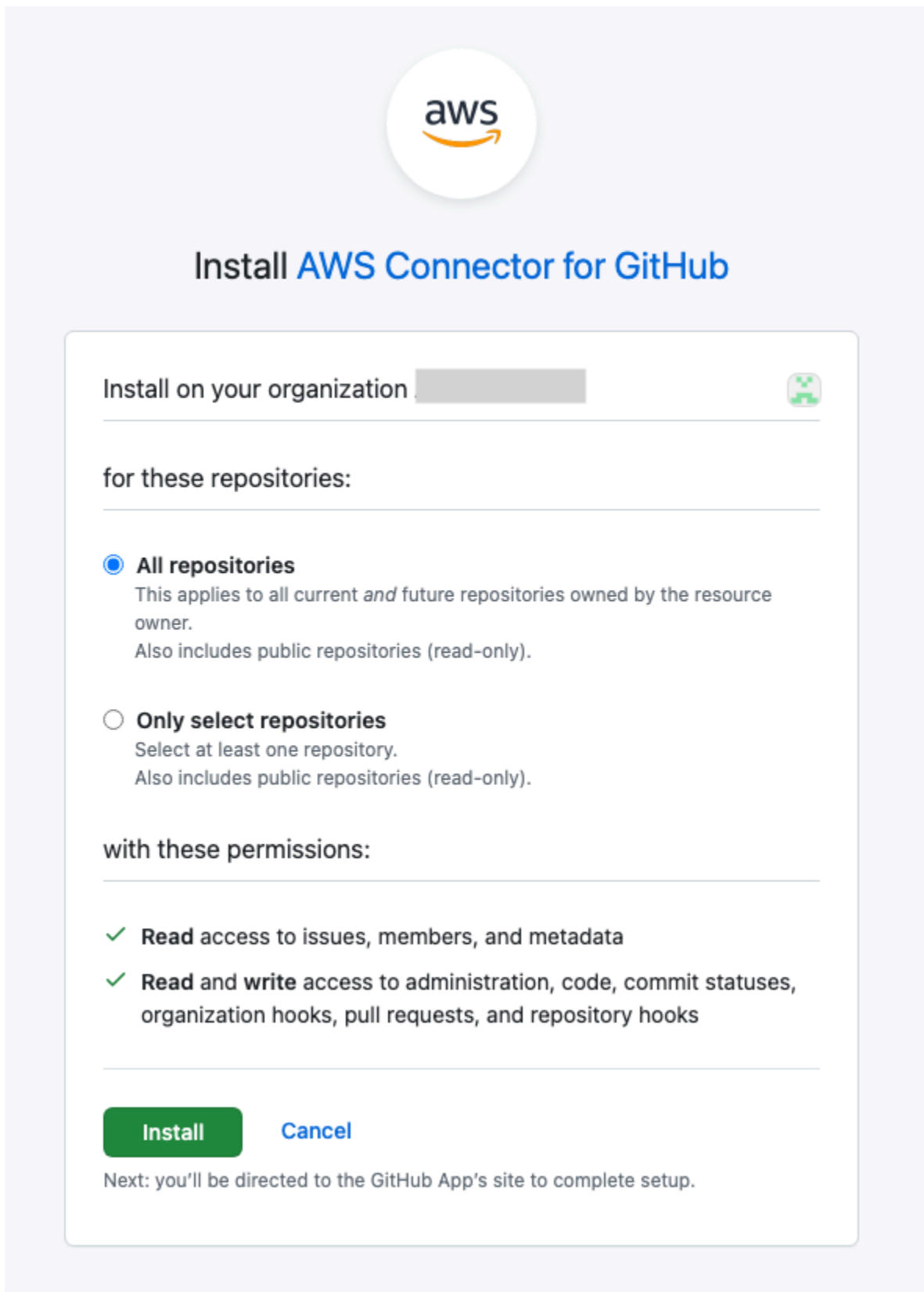
Anda menginstal satu aplikasi untuk semua koneksi Anda ke penyedia tertentu. Jika Anda telah menginstal AWS Connector for GitHub app, pilih dan lewati langkah ini.

- Pada GitHub halaman Install AWS Connector for, pilih akun tempat Anda ingin menginstal aplikasi.

**Note**

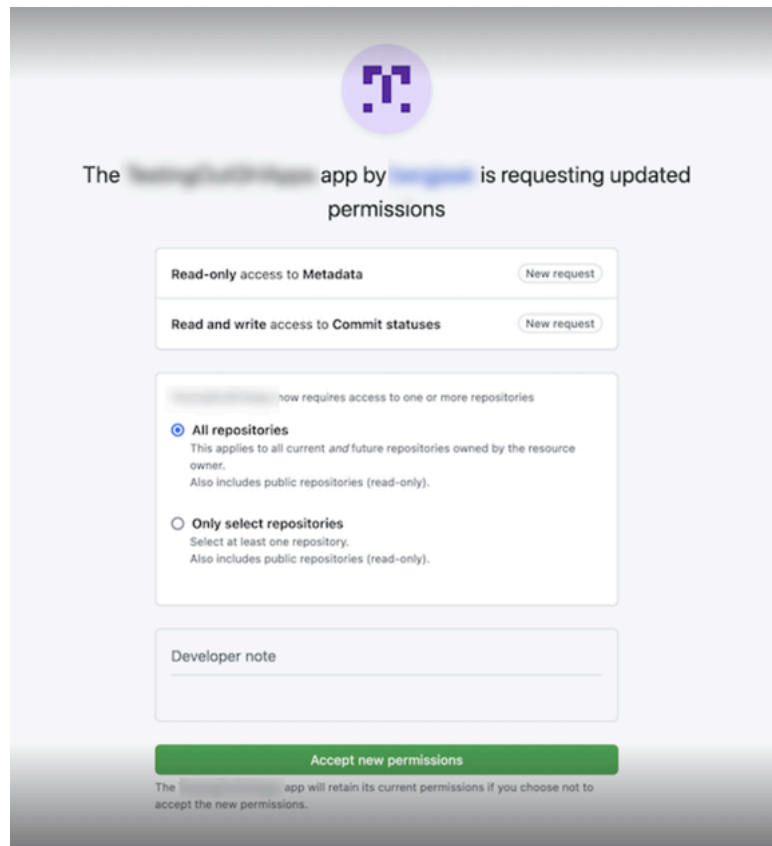
Anda hanya menginstal aplikasi sekali untuk setiap GitHub akun. Jika sebelumnya Anda menginstal aplikasi, Anda dapat memilih Konfigurasi untuk melanjutkan ke halaman modifikasi untuk instalasi aplikasi Anda, atau Anda dapat menggunakan tombol kembali untuk kembali ke konsol.

5. Pada GitHub halaman Install AWS Connector for, tinggalkan default, dan pilih Install.



Setelah langkah ini, halaman izin yang diperbarui mungkin ditampilkan. GitHub

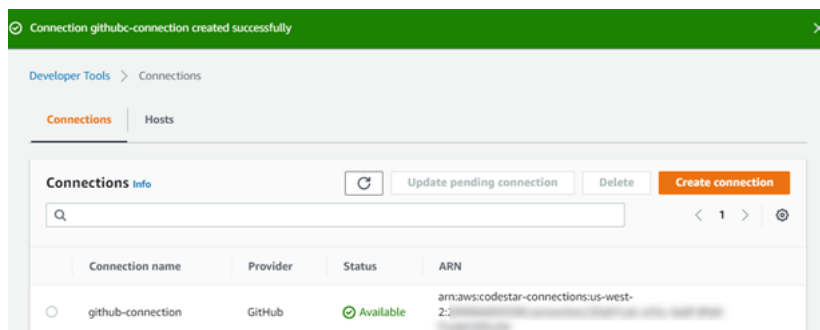
6. Jika halaman ditampilkan yang menunjukkan bahwa ada izin yang diperbarui untuk AWS Konektor untuk GitHub aplikasi, pilih Terima izin baru.



7. Anda dikembalikan ke GitHub halaman Connect to. ID koneksi untuk instalasi baru Anda muncul di GitHub Aplikasi. Pilih Hubungkan.

Lihat koneksi yang Anda buat

- Koneksi yang dibuat ditampilkan dalam daftar koneksi.



Buat koneksi ke GitHub (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk membuat koneksi ke GitHub.

Untuk melakukannya, gunakan perintah `create-connection`.

Important

Koneksi yang dibuat melalui AWS CLI atau AWS CloudFormation dalam PENDING status secara default. Setelah Anda membuat koneksi dengan CLI atau CloudFormation, gunakan konsol untuk mengedit koneksi untuk membuat statusnya AVAILABLE

Untuk membuat koneksi ke GitHub

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-connection` perintah, menentukan `--provider-type` dan `--connection-name` untuk koneksi Anda. Dalam contoh ini, nama penyedia pihak ketiga adalah GitHub dan nama koneksi yang ditentukan adalah `MyConnection`.

```
aws codeconnections create-connection --provider-type GitHub --connection-name
MyConnection
```

Jika berhasil, perintah ini mengembalikan informasi ARN koneksi seperti berikut ini.

```
{
  "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
}
```

2. Gunakan konsol untuk menyelesaikan koneksi. Untuk informasi selengkapnya, lihat [Memperbarui koneksi yang tertunda](#).

Membuat koneksi ke GitHub Enterprise Server

Anda menggunakan koneksi untuk mengaitkan AWS sumber daya Anda dengan repositori pihak ketiga. Anda dapat menggunakan Konsol Manajemen AWS atau AWS Command Line Interface (AWS CLI) untuk membuat koneksi ke GitHub Enterprise Server.

Koneksi hanya menyediakan akses ke repositori yang dimiliki oleh akun GitHub Enterprise Server yang digunakan selama pembuatan koneksi untuk mengotorisasi penginstalan aplikasi. GitHub

Sebelum Anda memulai:

- Anda harus sudah memiliki instance GitHub Enterprise Server dan repositori di dalamnya.
- Anda harus menjadi administrator instance GitHub Enterprise Server untuk membuat GitHub aplikasi dan membuat sumber daya host seperti yang ditunjukkan di bagian ini.

Important

Saat Anda menyiapkan host untuk GitHub Enterprise Server, titik akhir VPC untuk data peristiwa webhooks dibuat untuk Anda. Jika Anda membuat host sebelum 24 November 2020, dan Anda ingin menggunakan titik akhir PrivateLink webhook VPC, Anda harus terlebih dahulu [menghapus](#) host Anda dan kemudian [membuat](#) host baru.

Note

Untuk organisasi di Server GitHub Perusahaan atau yang GitLab dikelola sendiri, Anda tidak melewati host yang tersedia. Anda membuat host baru untuk setiap koneksi di organisasi Anda, dan Anda harus memastikan untuk memasukkan informasi yang sama di bidang jaringan (ID VPC, Subnet IDs, dan Grup Keamanan IDs) untuk host. Untuk informasi selengkapnya, lihat [Koneksi dan penyiapan host untuk penyedia terinstal yang mendukung organisasi](#).

Topik

- [Buat koneksi ke GitHub Enterprise Server \(konsol\)](#)
- [Buat koneksi ke GitHub Enterprise Server \(CLI\)](#)

Buat koneksi ke GitHub Enterprise Server (konsol)

Untuk membuat koneksi GitHub Enterprise Server, Anda memberikan informasi tentang tempat Server GitHub Perusahaan Anda diinstal dan mengotorisasi pembuatan koneksi dengan kredensi GitHub Enterprise Anda.

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan `codeconnections` ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Topik

- [Buat koneksi GitHub Enterprise Server Anda \(konsol\)](#)

Buat koneksi GitHub Enterprise Server Anda (konsol)

Untuk membuat koneksi ke GitHub Enterprise Server, siapkan URL server dan kredensi GitHub Enterprise Anda.

Untuk membuat host

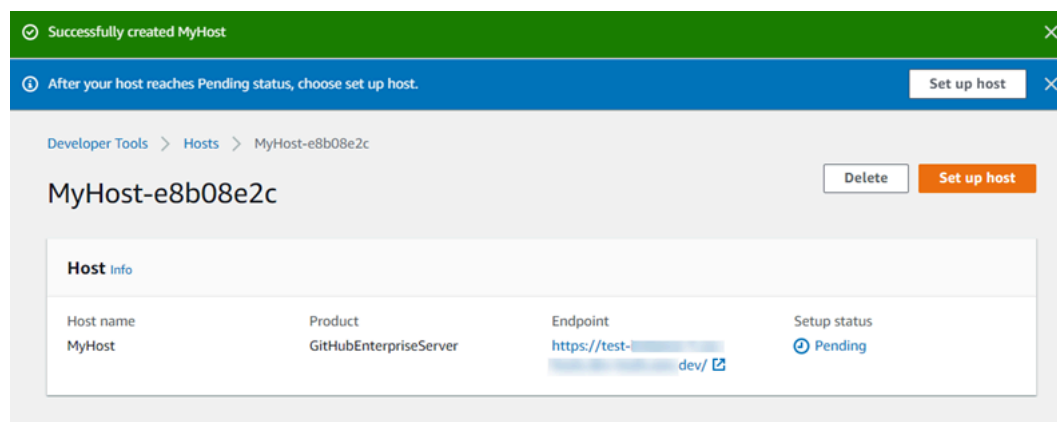
1. Masuk ke Konsol Manajemen AWS, dan buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pada tab Host, pilih Buat host.
3. Di Nama host, masukkan nama yang ingin Anda gunakan untuk host Anda.
4. Di Pilih penyedia, pilih salah satu dari berikut ini:
 - GitHub Server Perusahaan
 - GitLab dikelola sendiri
5. Di URL, masukkan titik akhir untuk infrastruktur tempat penyedia Anda diinstal.
6. Jika server Anda dikonfigurasi dalam Amazon VPC dan Anda ingin terhubung dengan VPC Anda, pilih Gunakan VPC. Jika tidak, pilih Tanpa VPC.
7. Jika Anda telah meluncurkan instans Anda ke Amazon VPC dan Anda ingin terhubung dengan VPC Anda, pilih Gunakan VPC dan selesaikan yang berikut ini.
 - a. Di ID VPC, pilih ID VPC anda. Pastikan untuk memilih VPC untuk infrastruktur tempat instans Anda diinstal atau VPC dengan akses ke instans Anda melalui VPN atau Direct Connect.
 - b. Jika Anda memiliki VPC pribadi yang dikonfigurasi, dan Anda telah mengonfigurasi instans Anda untuk melakukan validasi TLS menggunakan otoritas sertifikat non-publik, dalam sertifikat TLS, masukkan ID sertifikat Anda. Nilai Sertifikat TLS adalah kunci publik sertifikat.

- Pilih Buat host.
- Setelah halaman detail host ditampilkan, status host berubah saat host dibuat.

Note

Jika penyiapan host Anda menyertakan konfigurasi VPC, tunggu beberapa menit untuk penyediaan komponen jaringan host.

Tunggu host Anda mencapai status Tertunda, dan kemudian selesaikan penyiapan. Untuk informasi lebih lanjut, lihat [Menyiapkan host yang tertunda](#).



Langkah 2: Buat koneksi Anda ke GitHub Enterprise Server (konsol)

- Masuk ke Konsol Manajemen AWS dan buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
- Pilih Pengaturan > Koneksi, lalu pilih Buat koneksi.
- Untuk membuat sambungan ke repositori GitHub Enterprise Server yang diinstal, pilih GitHub Enterprise Server.

Connect ke GitHub Enterprise Server

- Di Nama koneksi, masukkan nama untuk koneksi Anda.

Developer Tools > Connections > Create connection

Create a connection Info

Select a provider

Bitbucket GitHub GitHub Enterprise Server

Connection Settings Info

Connection name
Give your connection a name.

URL
The endpoint of the server to connect to.

Use a VPC
If your GitHub Enterprise Server is only accessible in a VPC, configure details here. Otherwise, skip this step.
Complete these steps in the same AWS Region as your VPC.

Cancel

2. Di URL, masukkan titik akhir untuk server Anda.

Note

Jika URL yang disediakan telah digunakan untuk menyiapkan Server GitHub Perusahaan untuk koneksi, Anda akan diminta untuk memilih ARN sumber daya host yang dibuat sebelumnya untuk titik akhir tersebut.

3. (Opsional) Jika Anda telah meluncurkan server Anda ke VPC Amazon dan Anda ingin terhubung dengan VPC Anda, pilih Gunakan VPC dan selesaikan yang berikut ini.

Note

Untuk organisasi di Server GitHub Perusahaan atau yang GitLab dikelola sendiri, Anda tidak melewati host yang tersedia. Anda membuat host baru untuk setiap koneksi di organisasi Anda, dan Anda harus memastikan untuk memasukkan informasi yang sama di bidang jaringan (ID VPC, Subnet IDs, dan Grup Keamanan IDs) untuk host. Untuk

informasi selengkapnya, lihat [Koneksi dan penyiapan host untuk penyedia terinstal yang mendukung organisasi](#).

- a. Di ID VPC, pilih ID VPC anda. Pastikan untuk memilih VPC untuk infrastruktur tempat instans Server GitHub Perusahaan Anda diinstal atau VPC dengan akses ke instance Server GitHub Perusahaan Anda melalui VPN atau Direct Connect.
- b. Pada ID subnet, pilih Tambahkan. Di bidang, pilih ID subnet yang ingin Anda gunakan untuk host Anda. Anda dapat memilih hingga 10 subnet.

Pastikan untuk memilih subnet untuk infrastruktur tempat instans GitHub Enterprise Server Anda diinstal atau subnet dengan akses ke instance GitHub Enterprise Server yang diinstal melalui VPN atau Direct Connect.

- c. Di bawah Grup keamanan IDs, pilih Tambah. Di bidang, pilih grup keamanan yang ingin Anda gunakan untuk host Anda. Anda dapat memilih hingga 10 grup keamanan.

Pastikan untuk memilih grup keamanan untuk infrastruktur tempat instans Server GitHub Perusahaan Anda diinstal atau grup keamanan dengan akses ke instans Server GitHub Enterprise yang diinstal melalui VPN atau Direct Connect.

- d. Jika Anda memiliki VPC pribadi yang dikonfigurasi, dan Anda telah mengonfigurasi instance Server GitHub Perusahaan Anda untuk melakukan validasi TLS menggunakan otoritas sertifikat non-publik, dalam sertifikat TLS, masukkan ID sertifikat Anda. Nilai Sertifikat TLS harus menjadi kunci publik sertifikat.

VPC ID

Choose the VPC in which your GitHub Enterprise Server is configured.

Subnet IDs

Choose the subnet or subnets for the VPC in which your GitHub Enterprise Server is configured.

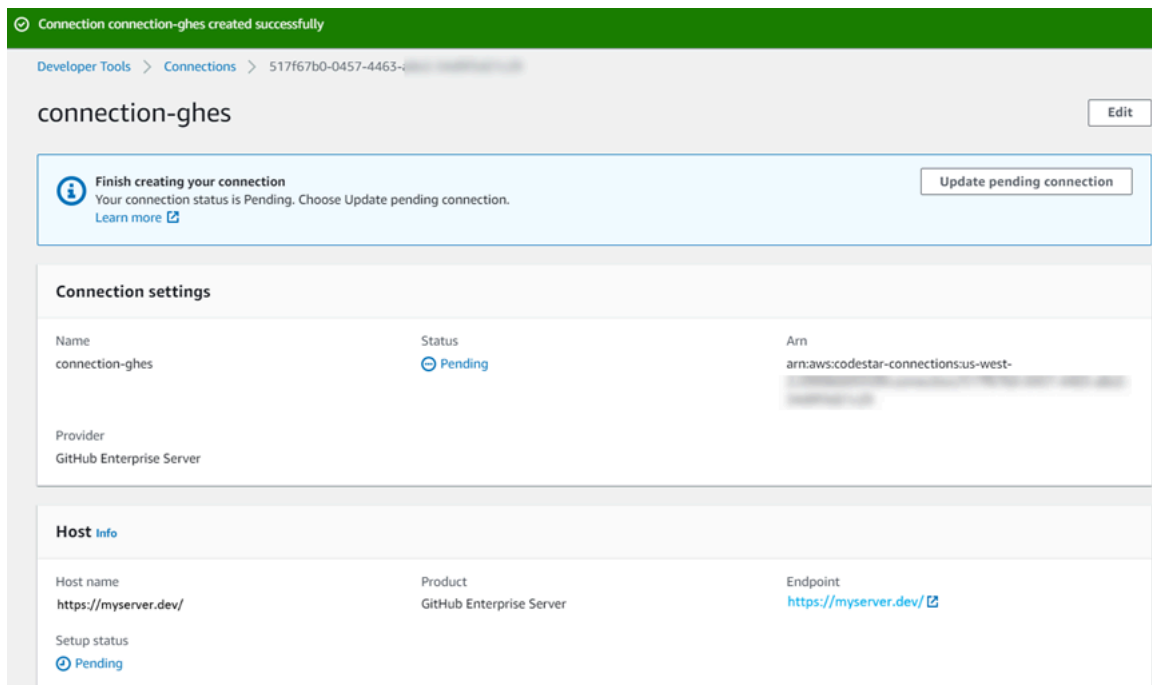
Subnet ID**Security group IDs**

Choose the security group or groups for the VPC in which your GitHub Enterprise Server is configured.

Security group ID**TLS certificate - optional**

If you have a private certificate authority behind a VPC or you are using a self-signed certificate paste the TLS certificate here.

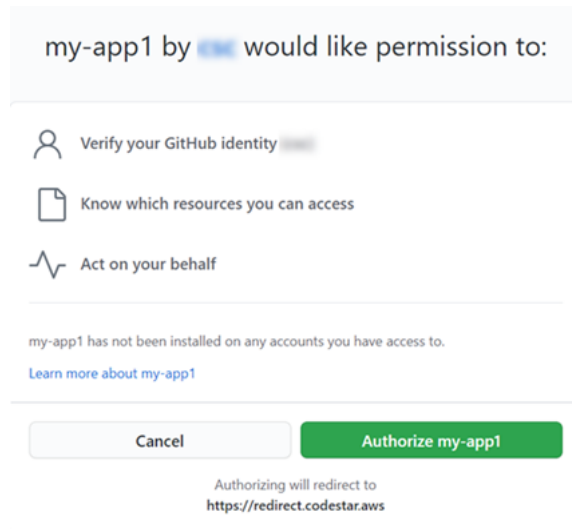
- Pilih Connect to GitHub Enterprise Server. Koneksi yang dibuat ditampilkan dengan status Tertunda. Sumber daya host dibuat untuk koneksi dengan informasi server yang Anda berikan. Untuk nama host, URL digunakan.
- Pilih Perbarui koneksi tertunda.



6. Jika diminta, pada halaman login GitHub Enterprise, masuk dengan kredensi GitHub Enterprise Anda.
7. Pada halaman Buat GitHub Aplikasi, pilih nama untuk aplikasi Anda.

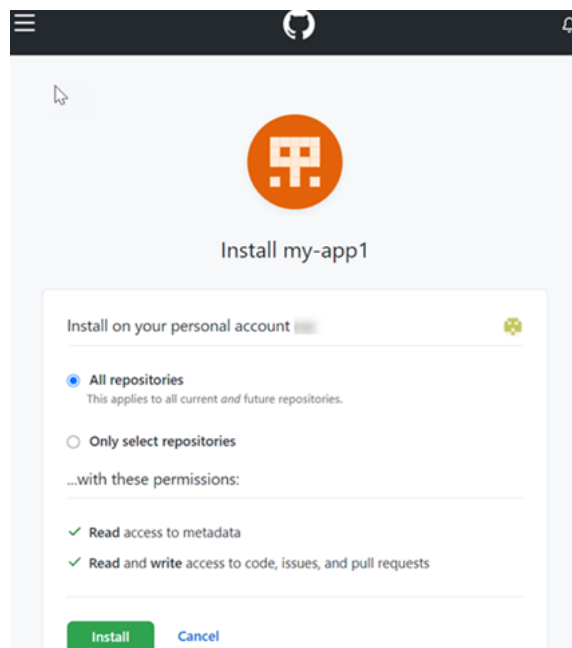


8. <app-name> Pada halaman GitHub otorisasi, pilih Otorisasi.



9. Pada halaman instalasi aplikasi, sebuah pesan menunjukkan bahwa aplikasi konektor siap untuk diinstal. Jika Anda memiliki beberapa organisasi, Anda mungkin diminta untuk memilih organisasi tempat Anda ingin menginstal aplikasi.

Pilih pengaturan repositori tempat Anda ingin menginstal aplikasi. Pilih Install.



10. Halaman koneksi yang menampilkan koneksi yang dibuat dalam status Tersedia.

Buat koneksi ke GitHub Enterprise Server (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk membuat koneksi.

Untuk melakukan ini, gunakan `create-host` dan `create-connection` perintah.

Important

Koneksi yang dibuat melalui AWS CLI atau AWS CloudFormation dalam PENDING status secara default. Setelah Anda membuat koneksi dengan CLI atau CloudFormation, gunakan konsol untuk mengedit koneksi untuk membuat statusnya. AVAILABLE

Langkah 1: Untuk membuat host untuk GitHub Enterprise Server (CLI)

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-host` perintah, menentukan, `--name`, `--provider-type`, dan `--provider-endpoint` untuk koneksi Anda. Dalam contoh ini, nama penyedia pihak ketiga adalah `GitHubEnterpriseServer` dan titik akhir adalah `my-instance.dev`.

```
aws codeconnections create-host --name MyHost --provider-type
GitHubEnterpriseServer --provider-endpoint "https://my-instance.dev"
```

Jika berhasil, perintah ini mengembalikan informasi Amazon Resource Name (ARN) host seperti berikut ini.

```
{
  "HostArn": "arn:aws:codeconnections:us-west-2:account_id:host/My-Host-28aef605"
}
```

Setelah langkah ini, host dalam status PENDING.

2. Gunakan konsol untuk menyelesaikan persiapan host dan memindahkan host ke status Available. Untuk informasi selengkapnya, lihat [Menyiapkan host yang tertunda](#).

Langkah 2: Untuk mengatur host yang tertunda di konsol

1. Masuk ke Konsol Manajemen AWS dan buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Gunakan konsol untuk menyelesaikan persiapan host dan memindahkan host ke status Available. Lihat [Menyiapkan host yang tertunda](#).

Langkah 3: Untuk membuat koneksi untuk GitHub Enterprise Server (CLI)

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-connection` perintah, menentukan `--host-arn` dan `--connection-name` untuk koneksi Anda.

```
aws codeconnections create-connection --host-arn arn:aws:codeconnections:us-west-2:account_id:host/MyHost-234EXAMPLE --connection-name MyConnection
```

Jika berhasil, perintah ini mengembalikan informasi ARN koneksi seperti berikut ini.

```
{
  "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/aEXAMPLE-8aad"
}
```

2. Gunakan konsol untuk mengatur koneksi yang tertunda. Untuk informasi selengkapnya, lihat [Memperbarui koneksi yang tertunda](#).

Langkah 4: Untuk menyelesaikan koneksi untuk GitHub Enterprise Server di konsol

1. Masuk ke Konsol Manajemen AWS dan buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Gunakan konsol untuk mengatur koneksi yang tertunda dan memindahkan koneksi ke Available status. Untuk informasi selengkapnya, lihat [Memperbarui koneksi yang tertunda](#).

Buat koneksi ke GitLab


Anda dapat menggunakan Konsol Manajemen AWS or the AWS Command Line Interface (AWS CLI) untuk membuat koneksi ke repositori yang dihosting di gitlab.com.

Note


Dengan mengotorisasi instalasi koneksi ini di GitLab, Anda memberikan izin layanan kami untuk memproses data Anda, dan Anda dapat mencabut izin kapan saja dengan menghapus instalasi aplikasi.

Sebelum Anda memulai:

- Anda harus sudah membuat akun dengan GitLab.

 Note

Koneksi hanya menyediakan akses untuk akun yang digunakan untuk membuat dan mengotorisasi koneksi.

 Note


Anda dapat membuat koneksi di mana Anda memiliki peran Pemilik GitLab, dan kemudian koneksi dapat digunakan dengan repositori dengan sumber daya seperti CodePipeline. Untuk repositori dalam grup, Anda tidak perlu menjadi pemilik grup.

Topik

- [Buat koneksi ke GitLab \(konsol\)](#)
- [Buat koneksi ke GitLab \(CLI\)](#)

Buat koneksi ke GitLab (konsol)

Anda dapat menggunakan konsol untuk membuat koneksi.

 Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan codeconnections ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Langkah 1: Buat koneksi Anda

1. Masuk ke Konsol Manajemen AWS, lalu buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan, lalu pilih Koneksi. Pilih Buat koneksi.

- Untuk membuat sambungan ke GitLab repositori, di bawah Pilih penyedia, pilih. GitLab Di Nama koneksi, masukkan nama untuk koneksi yang ingin Anda buat. Pilih Connect to GitLab.

Developer Tools > Connections > Create connection

Create a connection [Info](#)

Select a provider

Bitbucket

GitHub

GitHub Enterprise Server

GitLab

Create GitLab connection [Info](#)

Connection name

► **Tags - optional**

Connect to GitLab

- Saat halaman login untuk GitLab ditampilkan, masuk dengan kredensial Anda, lalu pilih Masuk.
- Halaman otorisasi ditampilkan dengan pesan yang meminta otorisasi untuk koneksi untuk mengakses akun Anda. GitLab

Pilih Izinkan.

Authorize **codestar-connections** to use your account?

An application called **codestar-connections** is requesting access to your GitLab account. This application was created by **Amazon AWS**. Please note that this application is not provided by GitLab and you should verify its authenticity before allowing access.

This application will be able to:

- **Access the authenticated user's API**
Grants complete read/write access to the API, including all groups and projects, the container registry, and the package registry.
- **Read the authenticated user's personal information**
Grants read-only access to the authenticated user's profile through the /user API endpoint, which includes username, public email, and full name. Also grants access to read-only API endpoints under /users.
- **Read Api**
Grants read access to the API, including all groups and projects, the container registry, and the package registry.
- **Allows read-only access to the repository**
Grants read-only access to repositories on private projects using Git-over-HTTP or the Repository Files API.
- **Allows read-write access to the repository**
Grants read-write access to repositories on private projects using Git-over-HTTP (not using the API).

Deny

Authorize

6. Browser kembali ke halaman konsol koneksi. Di bawah Buat GitLab koneksi, koneksi baru ditampilkan di Nama koneksi.
7. Pilih Connect to GitLab.

Setelah koneksi berhasil dibuat, spanduk sukses ditampilkan. Detail koneksi ditampilkan di halaman Pengaturan koneksi.

Buat koneksi ke GitLab (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk membuat koneksi.

Untuk melakukannya, gunakan perintah `create-connection`.

Important

Koneksi yang dibuat melalui AWS CLI atau AWS CloudFormation dalam PENDING status secara default. Setelah Anda membuat koneksi dengan CLI atau CloudFormation, gunakan konsol untuk mengedit koneksi untuk membuat statusnya. AVAILABLE

Untuk membuat koneksi ke GitLab

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-connection` perintah, menentukan `--provider-type` dan `--connection-name` untuk koneksi Anda. Dalam contoh ini, nama penyedia pihak ketiga adalah GitLab dan nama koneksi yang ditentukan adalah `MyConnection`.

```
aws codeconnections create-connection --provider-type GitLab --connection-name
MyConnection
```

Jika berhasil, perintah ini mengembalikan informasi ARN koneksi seperti berikut ini.

```
{
  "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
}
```

2. Gunakan konsol untuk menyelesaikan koneksi. Untuk informasi selengkapnya, lihat [Memperbarui koneksi yang tertunda](#).

Buat koneksi ke GitLab self-managed

Anda dapat membuat koneksi untuk GitLab Enterprise Edition atau GitLab Community Edition dengan instalasi yang dikelola sendiri.

Anda dapat menggunakan Konsol Manajemen AWS or the AWS Command Line Interface (AWS CLI) untuk membuat koneksi dan host untuk GitLab dikelola sendiri.

Note

Dengan mengotorisasi aplikasi koneksi ini dalam GitLab pengelolaan sendiri, Anda memberikan izin layanan kami untuk memproses data Anda, dan Anda dapat mencabut izin kapan saja dengan menghapus instalasi aplikasi.

Sebelum Anda membuat koneksi ke GitLab dikelola sendiri, Anda harus membuat host untuk digunakan untuk koneksi, seperti yang dijelaskan dalam langkah-langkah ini. Untuk ikhtisar alur kerja pembuatan host untuk penyedia yang diinstal, lihat [Alur kerja untuk membuat atau memperbarui host](#).

Anda dapat mengonfigurasi host Anda secara opsional dengan VPC. Untuk informasi selengkapnya tentang konfigurasi jaringan dan VPC untuk sumber daya host Anda, lihat prasyarat VPC di dan [\(Opsional\) Prasyarat: Konfigurasi VPC Jaringan atau Amazon untuk koneksi Anda Pemecahan masalah konfigurasi VPC untuk host Anda](#)

Sebelum Anda memulai:

- Anda harus sudah membuat akun dengan GitLab dan memiliki GitLab Enterprise Edition atau GitLab Community Edition dengan instalasi yang dikelola sendiri. Untuk informasi selengkapnya, lihat https://docs.gitlab.com/ee/subscriptions/self_managed/.

Note

Koneksi hanya menyediakan akses untuk akun yang digunakan untuk membuat dan mengotorisasi koneksi.

Note

Anda dapat membuat koneksi ke repositori tempat Anda memiliki peran Pemilik GitLab, dan kemudian koneksi dapat digunakan dengan sumber daya seperti. CodePipeline Untuk repositori dalam grup, Anda tidak perlu menjadi pemilik grup.

- Anda harus sudah membuat token akses GitLab pribadi (PAT) dengan izin cakupan bawah berikut saja:,. api admin_mode Untuk informasi lebih lanjut, lihat https://docs.gitlab.com/ee/user/profile/personal_access_tokens.html. Anda harus menjadi administrator untuk membuat dan menggunakan PAT.

Note

PAT Anda digunakan untuk mengotorisasi host dan tidak disimpan atau digunakan oleh koneksi. Untuk mengatur host, Anda dapat membuat PAT sementara dan kemudian setelah Anda mengatur host, Anda dapat menghapus PAT.

Note

Untuk organisasi di Server GitHub Perusahaan atau yang GitLab dikelola sendiri, Anda tidak melewati host yang tersedia. Anda membuat host baru untuk setiap koneksi di organisasi Anda, dan Anda harus memastikan untuk memasukkan informasi yang sama di bidang jaringan (ID VPC, Subnet IDs, dan Grup Keamanan IDs) untuk host. Untuk informasi selengkapnya, lihat [Koneksi dan penyiapan host untuk penyedia terinstal yang mendukung organisasi](#).

Topik

- [Buat koneksi ke GitLab self-managed \(konsol\)](#)
- [Buat koneksi ke GitLab self-managed \(CLI\)](#)

Buat koneksi ke GitLab self-managed (konsol)

Gunakan langkah-langkah ini untuk membuat host dan koneksi untuk GitLab dikelola sendiri di konsol. Untuk pertimbangan untuk menyiapkan host di VPC, lihat. [\(Opsional\) Prasyarat: Konfigurasi VPC Jaringan atau Amazon untuk koneksi Anda](#)

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan `codeconnections` ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Note

Anda membuat host untuk satu instalasi yang GitLab dikelola sendiri, dan kemudian Anda dapat mengelola satu atau lebih koneksi yang GitLab dikelola sendiri ke host tersebut.

Langkah 1: Buat host Anda


1. Masuk ke Konsol Manajemen AWS, lalu buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pada tab Host, pilih Buat host.
3. Di Nama host, masukkan nama yang ingin Anda gunakan untuk host Anda.
4. Di Pilih penyedia, pilih GitLabdikelola sendiri.
5. Di URL, masukkan titik akhir untuk infrastruktur tempat penyedia Anda diinstal.
6. Jika server Anda dikonfigurasi dalam Amazon VPC dan Anda ingin terhubung dengan VPC Anda, pilih Gunakan VPC. Jika tidak, pilih Tanpa VPC.
7. (Opsional) Jika Anda telah meluncurkan host Anda ke VPC Amazon dan Anda ingin terhubung dengan VPC Anda, pilih Gunakan VPC dan selesaikan yang berikut ini.

Note

Untuk organisasi di Server GitHub Perusahaan atau yang GitLab dikelola sendiri, Anda tidak melewati host yang tersedia. Anda membuat host baru untuk setiap koneksi di organisasi Anda, dan Anda harus memastikan untuk memasukkan informasi yang sama di bidang jaringan (ID VPC, Subnet IDs, dan Grup Keamanan IDs) untuk host. Untuk

informasi selengkapnya, lihat [Koneksi dan penyiapan host untuk penyedia terinstal yang mendukung organisasi](#).

- a. Di ID VPC, pilih ID VPC anda. Pastikan untuk memilih VPC untuk infrastruktur tempat host Anda diinstal atau VPC dengan akses ke instans Anda melalui VPN atau Direct Connect.
 - b. Jika Anda memiliki VPC pribadi yang dikonfigurasi, dan Anda telah mengonfigurasi host Anda untuk melakukan validasi TLS menggunakan otoritas sertifikat non-publik, dalam sertifikat TLS, masukkan ID sertifikat Anda. Nilai Sertifikat TLS adalah kunci publik sertifikat.
8. Pilih Buat host.
 9. Setelah halaman detail host ditampilkan, status host berubah saat host dibuat.

 Note

Jika penyiapan host Anda menyertakan konfigurasi VPC, tunggu beberapa menit untuk penyediaan komponen jaringan host.

Tunggu host Anda mencapai status Tertunda, dan kemudian selesaikan penyiapan. Untuk informasi selengkapnya, lihat [Menyiapkan host yang tertunda](#).

Developer Tools > Hosts > dkhost-f7af82a

host-f7af82a Delete Edit Set up host

Host Info

Host name	Product	Setup status
host	GitLab self-managed	Pending
Arn	Endpoint	
arn:aws:iam::1:45...	https://us-west-1.amazonaws.com	

Host tags Info

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to help manage and secure your resources or to help track costs.

Edit

< 1 > ⚙️

Key	Value
No results	
There are no results to display.	

Add tag

Langkah 2: Siapkan host Anda yang tertunda

1. Pilih Siapkan host.
2. A Menyiapkan tampilan *host_name* halaman. Di Menyediakan token akses pribadi, berikan GitLab PAT Anda dengan izin cakupan bawah berikut saja: dan. api admin_mode

i Note

Hanya administrator yang dapat membuat dan menggunakan PAT.

Set up myhostgl

Provide personal access token

To set up GitLab self-managed, provide your personal access token from GitLab. The personal access token is required to have the following scoped-down permissions only: api.

- 3. Setelah host Anda berhasil terdaftar, halaman detail host muncul dan menunjukkan bahwa status host Tersedia.

:glhost-5

Host [Info](#)

Host name	Product	Setup status
:glhost	GitLab self-managed	✔ Available

Arn	Endpoint
[Redacted]	[Redacted]

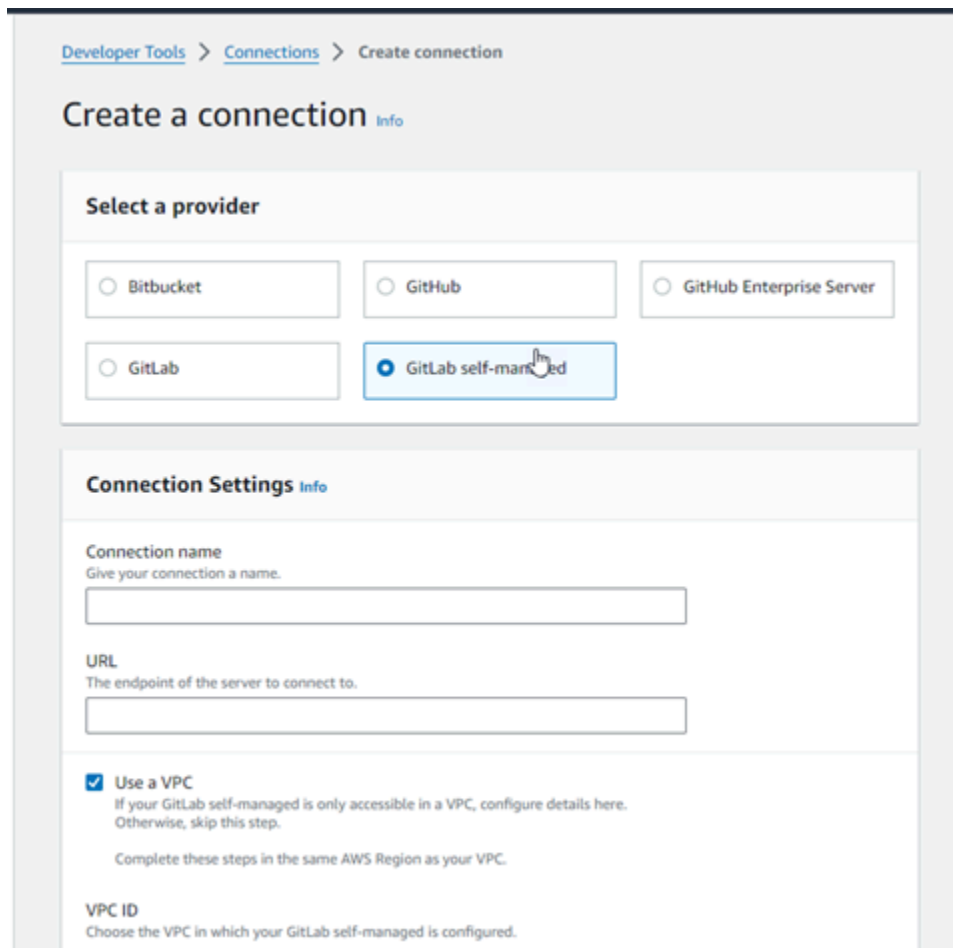
Host tags [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to help manage and secure your resources or to help track costs.

< 1 >

Langkah 3: Buat koneksi Anda

1. Masuk ke Konsol Manajemen AWS, lalu buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan, lalu pilih Koneksi. Pilih Buat koneksi.
3. Untuk membuat sambungan ke GitLab repositori, di bawah Pilih penyedia, pilih GitLab dikelola sendiri. Di Nama koneksi, masukkan nama untuk koneksi yang ingin Anda buat.



The screenshot shows the 'Create a connection' page in the AWS Developer Tools console. The breadcrumb trail is 'Developer Tools > Connections > Create connection'. The main heading is 'Create a connection' with an 'Info' icon. Under 'Select a provider', there are five radio button options: Bitbucket, GitHub, GitHub Enterprise Server, GitLab, and GitLab self-managed (which is selected). Below this is the 'Connection Settings' section with an 'Info' icon. It contains a 'Connection name' field with the instruction 'Give your connection a name.', a 'URL' field with the instruction 'The endpoint of the server to connect to.', a checked checkbox for 'Use a VPC' with the instruction 'If your GitLab self-managed is only accessible in a VPC, configure details here. Otherwise, skip this step.' and the note 'Complete these steps in the same AWS Region as your VPC.', and a 'VPC ID' field with the instruction 'Choose the VPC in which your GitLab self-managed is configured.'

4. Di URL, masukkan titik akhir untuk server Anda.
5. Jika Anda telah meluncurkan server Anda ke Amazon VPC dan Anda ingin terhubung dengan VPC Anda, pilih Gunakan VPC dan selesaikan yang berikut ini.
 - a. Di ID VPC, pilih ID VPC anda. Pastikan untuk memilih VPC untuk infrastruktur tempat host Anda diinstal atau VPC dengan akses ke host Anda melalui VPN atau Direct Connect.
 - b. Pada ID subnet, pilih Tambahkan. Di bidang, pilih ID subnet yang ingin Anda gunakan untuk host Anda. Anda dapat memilih hingga 10 subnet.

Pastikan untuk memilih subnet untuk infrastruktur tempat host Anda diinstal atau subnet dengan akses ke host yang diinstal melalui VPN atau Direct Connect.

- c. Di bawah Grup keamanan IDs, pilih Tambah. Di bidang, pilih grup keamanan yang ingin Anda gunakan untuk host Anda. Anda dapat memilih hingga 10 grup keamanan.

Pastikan untuk memilih grup keamanan untuk infrastruktur tempat host Anda diinstal atau grup keamanan dengan akses ke host terinstal Anda melalui VPN atau Direct Connect.

- d. Jika Anda memiliki VPC pribadi yang dikonfigurasi, dan Anda telah mengonfigurasi host Anda untuk melakukan validasi TLS menggunakan otoritas sertifikat non-publik, dalam sertifikat TLS, masukkan ID sertifikat Anda. Nilai Sertifikat TLS harus menjadi kunci publik sertifikat.
6. Pilih Connect to GitLab self-managed. Koneksi yang dibuat ditampilkan dengan status Tertunda. Sumber daya host dibuat untuk koneksi dengan informasi server yang Anda berikan. Untuk nama host, URL digunakan.
 7. Pilih Perbarui koneksi tertunda.
 8. Saat halaman login untuk GitLab ditampilkan, masuk dengan kredensial Anda, lalu pilih Masuk.
 9. Halaman otorisasi ditampilkan dengan pesan yang meminta otorisasi untuk koneksi untuk mengakses akun Anda. GitLab

Pilih Izinkan.

10. Browser kembali ke halaman konsol koneksi. Di bawah Buat GitLab koneksi, koneksi baru ditampilkan di Nama koneksi.
11. Pilih Connect to GitLab self-managed.

Setelah koneksi berhasil dibuat, spanduk sukses ditampilkan. Detail koneksi ditampilkan di halaman Pengaturan koneksi.

Buat koneksi ke GitLab self-managed (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk membuat host dan koneksi untuk GitLab dikelola sendiri.

Untuk melakukan ini, gunakan `create-host` dan `create-connection` perintah.

⚠ Important

Koneksi yang dibuat melalui AWS CLI atau AWS CloudFormation dalam PENDING status secara default. Setelah Anda membuat koneksi dengan CLI atau CloudFormation, gunakan konsol untuk mengedit koneksi untuk membuat statusnya. AVAILABLE

Langkah 1: Untuk membuat host untuk GitLab dikelola sendiri (CLI)

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-host` perintah, menentukan, `--name`, `--provider-type`, dan `--provider-endpoint` untuk koneksi Anda. Dalam contoh ini, nama penyedia pihak ketiga adalah `GitLabSelfManaged` dan titik akhir adalah `my-instance.dev`.

```
aws codeconnections create-host --name MyHost --provider-type GitLabSelfManaged --
provider-endpoint "https://my-instance.dev"
```

Jika berhasil, perintah ini mengembalikan informasi Amazon Resource Name (ARN) host seperti berikut ini.

```
{
  "HostArn": "arn:aws:codeconnections:us-west-2:account_id:host/My-Host-28aef605"
}
```

Setelah langkah ini, host dalam status PENDING.

2. Gunakan konsol untuk menyelesaikan persiapan host dan pindahkan host ke Available status pada langkah berikut.

Langkah 2: Untuk mengatur host yang tertunda di konsol

1. Masuk ke Konsol Manajemen AWS dan buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Gunakan konsol untuk menyelesaikan persiapan host dan memindahkan host ke status Available. Lihat [Menyiapkan host yang tertunda](#).

Langkah 3: Untuk membuat koneksi untuk GitLab dikelola sendiri (CLI)

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-connection` perintah, menentukan `--host-arn` dan `--connection-name` untuk koneksi Anda.

```
aws codeconnections create-connection --host-arn arn:aws:codeconnections:us-west-2:account_id:host/MyHost-234EXAMPLE --connection-name MyConnection
```

Jika berhasil, perintah ini mengembalikan informasi ARN koneksi seperti berikut ini.

```
{
  "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/aEXAMPLE-8aad"
}
```

2. Gunakan konsol untuk mengatur koneksi yang tertunda di langkah berikut.

Langkah 4: Untuk menyelesaikan koneksi untuk GitLab dikelola sendiri di konsol

1. Masuk ke Konsol Manajemen AWS dan buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Gunakan konsol untuk mengatur koneksi yang tertunda dan memindahkan koneksi ke Available status. Untuk informasi selengkapnya, lihat [Memperbarui koneksi yang tertunda](#).

Memperbarui koneksi yang tertunda

Koneksi yang dibuat melalui AWS Command Line Interface (AWS CLI) atau AWS CloudFormation dalam PENDING status secara default. Setelah Anda membuat koneksi dengan AWS CLI atau CloudFormation, gunakan konsol untuk memperbarui koneksi untuk membuat statusnya AVAILABLE.

Note

Anda harus menggunakan konsol untuk memperbarui koneksi yang tertunda. Anda tidak dapat memperbarui koneksi yang tertunda menggunakan AWS CLI.

Pertama kali Anda menggunakan konsol untuk menambahkan koneksi baru ke penyedia pihak ketiga, Anda harus menyelesaikan OAuth jabat tangan dengan penyedia pihak ketiga menggunakan instalasi yang terkait dengan koneksi Anda.

Anda dapat menggunakan konsol Alat Developer untuk menyelesaikan koneksi yang tertunda.

Untuk menyelesaikan koneksi

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.

2. Pilih Pengaturan > Koneksi.

Nama-nama semua koneksi yang terkait dengan AWS akun Anda ditampilkan.

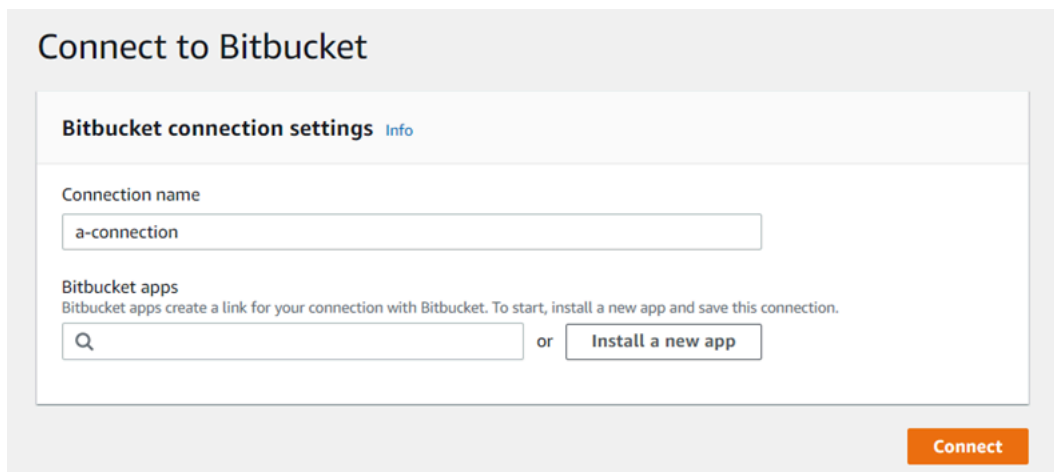
3. Di Nama, pilih nama koneksi yang tertunda yang ingin Anda perbarui.

Perbarui koneksi tertunda diaktifkan saat Anda memilih koneksi dengan status Tertunda.

4. Pilih Perbarui koneksi yang tertunda.

5. Pada halaman Hubungkan ke Bitbucket, di Nama koneksi, verifikasi nama koneksi Anda.

Pada Aplikasi Bitbucket, pilih penginstalan aplikasi, atau pilih Instal aplikasi baru untuk membuatnya.



Connect to Bitbucket

Bitbucket connection settings [Info](#)

Connection name

a-connection

Bitbucket apps

Bitbucket apps create a link for your connection with Bitbucket. To start, install a new app and save this connection.

or

6. Pada halaman instalasi aplikasi, sebuah pesan menunjukkan bahwa AWS CodeStar aplikasi sedang mencoba untuk terhubung ke akun Bitbucket Anda. Pilih Berikan akses.



AWS CodeStar requests access

This app is hosted at <https://codestar-connections.webhooks.aws>

Read your account information

Read your repositories and their pull requests

Administer your repositories

Read and modify your repositories

Authorize for

Allow AWS CodeStar to do this?

This 3rd party vendor has not provided a privacy policy or terms of use.

Atlassian's Privacy Policy is not applicable to the use of this App.

Grant access Cancel

7. ID koneksi untuk instalasi baru Anda ditampilkan. Pilih Selesaikan koneksi.

Daftar koneksi

Anda dapat menggunakan konsol Alat Pengembang atau `list-connections` perintah di AWS Command Line Interface (AWS CLI) untuk melihat daftar koneksi di akun Anda.

Daftar koneksi (konsol)

Untuk membuat daftar koneksi

1. Buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan > Koneksi.
3. Lihat nama, status, dan ARN untuk koneksi Anda.

Daftar koneksi (CLI)

Anda dapat menggunakan daftar koneksi Anda AWS CLI ke repositori kode pihak ketiga. Untuk koneksi yang terkait dengan sumber daya host, seperti koneksi ke GitHub Enterprise Server, output juga mengembalikan ARN host.

Untuk melakukannya, gunakan perintah `list-connections`.

Untuk membuat daftar koneksi

- Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows), dan gunakan AWS CLI untuk menjalankan perintah. `list-connections`

```
aws codeconnections list-connections --provider-type Bitbucket
--max-results 5 --next-token: next-token
```

Perintah ini mengembalikan output berikut.

```
{
  "Connections": [
    {
      "ConnectionName": "my-connection",
      "ProviderType": "Bitbucket",
      "Status": "PENDING",
      "ARN": "arn:aws:codeconnections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
      "OwnerAccountId": "account_id"
    },
    {
      "ConnectionName": "my-other-connection",
      "ProviderType": "Bitbucket",
      "Status": "AVAILABLE",
      "ARN": "arn:aws:codeconnections:us-west-2:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
      "OwnerAccountId": "account_id"
    }
  ],
  "NextToken": "next-token"
}
```

Menghapus koneksi

Anda dapat menggunakan konsol Alat Pengembang atau delete-connection perintah di AWS Command Line Interface (AWS CLI) untuk menghapus koneksi.


Topik

- [Menghapus koneksi \(konsol\)](#)
- [Menghapus koneksi \(CLI\)](#)

Menghapus koneksi (konsol)

Untuk menghapus koneksi

1. Buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan > Koneksi.
3. Di Nama koneksi, pilih nama koneksi yang ingin Anda hapus.
4. Pilih Hapus.
5. Masukkan **delete** di bidang untuk mengonfirmasi, lalu pilih Hapus.


 Important

Tindakan ini tidak dapat dibatalkan.

Menghapus koneksi (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menghapus koneksi.

Untuk melakukannya, gunakan perintah delete-connection.

 Important

Setelah Anda menjalankan perintah tersebut, koneksi dihapus. Tidak ada kotak dialog konfirmasi yang ditampilkan. Anda dapat membuat koneksi baru, tetapi Amazon Resource Name (ARN) tidak pernah digunakan kembali.

Untuk menghapus koneksi

- Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan delete-connection perintah, menentukan ARN dari koneksi yang ingin Anda hapus.

```
aws codeconnections delete-connection --connection-arn arn:aws:codeconnections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Perintah ini tidak mengembalikan apa pun.

Menandai sumber daya koneksi

Tag adalah label atribut kustom yang Anda atau AWS tetapkan ke AWS sumber daya. Setiap AWS tag memiliki dua bagian:

- Sebuah kunci tag (misalnya, `CostCenter`, `Environment`, atau `Project`). Kunci tanda peka terhadap huruf besar dan kecil.
- Bidang opsional yang dikenal sebagai nilai tag (misalnya, `111122223333`, `Production`, atau nama tim). Mengabaikan nilai tag sama dengan menggunakan rangkaian kosong. Seperti kunci tanda, nilai tanda peka huruf besar dan kecil.

Bersama-sama ini dikenal sebagai pasangan nilai kunci.

Anda dapat menggunakan konsol atau CLI untuk menandai sumber daya.

Anda dapat menandai jenis sumber daya berikut di AWS CodeConnections:

- Koneksi
- Host

Langkah-langkah ini mengasumsikan bahwa Anda telah menginstal versi terbaru AWS CLI atau diperbarui ke versi saat ini. Untuk informasi selengkapnya, lihat [Menginstal AWS CLI](#) dalam Panduan Pengguna AWS Command Line Interface .

Selain mengidentifikasi, mengatur, dan melacak sumber daya Anda dengan tag, Anda dapat menggunakan kebijakan tag dalam AWS Identity and Access Management (IAM) untuk membantu mengontrol siapa yang dapat melihat dan berinteraksi dengan sumber daya Anda. Untuk

contoh kebijakan akses berbasis tag, lihat [Menggunakan tag untuk mengontrol akses ke AWS CodeConnections sumber daya](#).

Topik

- [Menandai sumber daya \(konsol\)](#)
- [Tanda sumber daya \(CLI\)](#)

Menandai sumber daya (konsol)

Anda dapat menggunakan konsol untuk menambah, memperbarui, atau menghapus tanda pada sumber daya koneksi.

Topik

- [Menambahkan tanda ke sumber daya koneksi \(konsol\)](#)
- [Melihat tanda untuk sumber daya koneksi \(konsol\)](#)
- [Edit tanda untuk sumber daya koneksi \(konsol\)](#)
- [Hapus tanda dari sumber daya koneksi \(konsol\)](#)

Menambahkan tanda ke sumber daya koneksi (konsol)

Anda dapat menggunakan konsol untuk menambahkan tanda ke koneksi atau host yang ada.

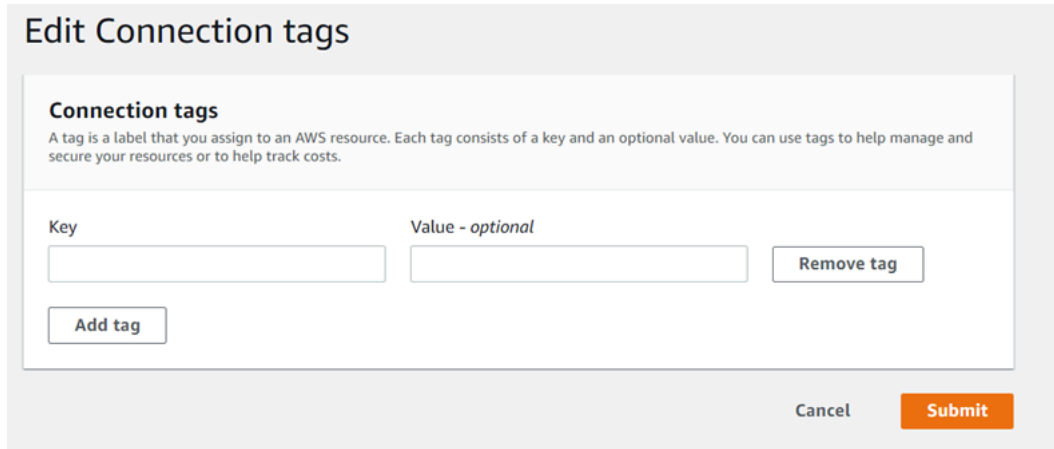
Note

Saat Anda membuat koneksi untuk penyedia yang diinstal seperti GitHub Enterprise Server, dan sumber daya host juga dibuat untuk Anda, tag selama pembuatan ditambahkan ke koneksi saja. Hal ini memungkinkan Anda untuk menandai host secara terpisah jika Anda ingin menggunakannya kembali untuk koneksi baru. Jika Anda ingin menambahkan tanda ke host, gunakan langkah-langkah di sini.

Untuk menambahkan tag untuk koneksi

1. Masuk ke konsol . Dari panel navigasi, pilih Pengaturan.
2. Pada Pengaturan, pilih Koneksi. Pilih tab Koneksi.
3. Pilih koneksi yang ingin Anda edit. Halaman pengaturan koneksi ditampilkan.
4. Pada Tanda koneksi, pilih Edit. Halaman Edit Tanda koneksi ditampilkan.

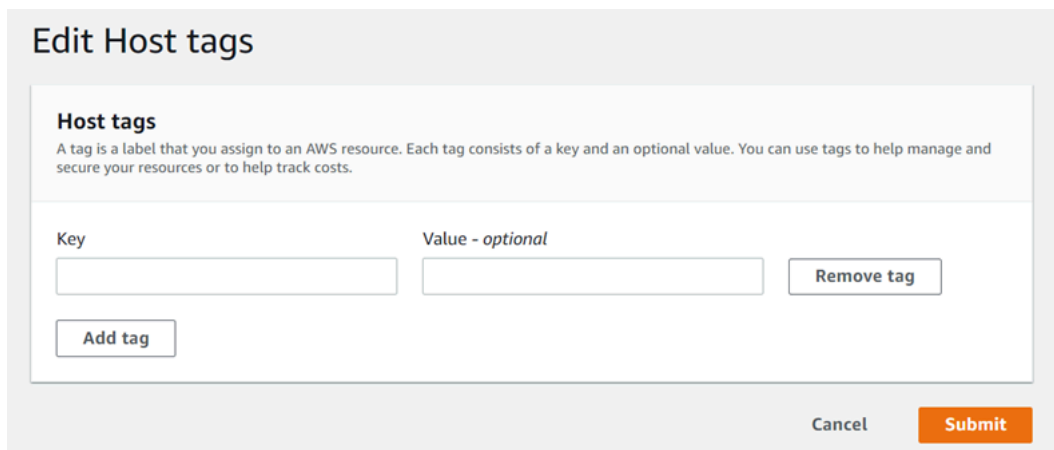
5. Di bidang Kunci dan Nilai, masukkan pasangan kunci untuk setiap kumpulan tanda yang ingin Anda tambahkan. (Bidang Nilai adalah bersifat opsional.) Contohnya, dalam Key (Kunci), masukkan **Project**. Dalam Value (Nilai), masukkan **ProjectA**.



6. (Opsional) Pilih Tambahkan tanda untuk menambahkan lebih banyak baris dan masukkan lebih banyak tanda.
7. Pilih Kirim. Tanda tercantum di bawah pengaturan koneksi.

Untuk menambahkan tag untuk host

1. Masuk ke konsol . Dari panel navigasi, pilih Pengaturan.
2. Pada Pengaturan, pilih Koneksi. Pilih tab Host.
3. Pilih host yang ingin Anda edit. Halaman pengaturan host ditampilkan.
4. Pada Tanda host, pilih Edit. Halaman Tanda host ditampilkan.
5. Di bidang Kunci dan Nilai, masukkan pasangan kunci untuk setiap kumpulan tanda yang ingin Anda tambahkan. (Bidang Nilai adalah bersifat opsional.) Contohnya, dalam Key (Kunci), masukkan **Project**. Dalam Value (Nilai), masukkan **ProjectA**.



6. (Opsional) Pilih Tambahkan tanda untuk menambahkan lebih banyak baris dan masukkan lebih banyak tanda untuk host.
7. Pilih Kirim. Tanda tercantum di bawah pengaturan host.

Melihat tanda untuk sumber daya koneksi (konsol)

Anda dapat menggunakan konsol untuk melihat tanda untuk sumber daya yang ada.

Untuk melihat tag untuk koneksi

1. Masuk ke konsol . Dari panel navigasi, pilih Pengaturan.
2. Pada Pengaturan, pilih Koneksi. Pilih tab Koneksi.
3. Pilih koneksi yang ingin Anda lihat. Halaman pengaturan koneksi ditampilkan.
4. Pada Tanda koneksi, lihat tanda untuk koneksi di bawah kolom Kunci dan Nilai.

Untuk melihat tag untuk host

1. Masuk ke konsol . Dari panel navigasi, pilih Pengaturan.
2. Pada Pengaturan, pilih Koneksi. Pilih tab Host.
3. Pilih host yang ingin Anda lihat.
4. Pada Tanda host, lihat tanda untuk host di bawah kolom Kunci dan Nilai.

Edit tanda untuk sumber daya koneksi (konsol)

Anda dapat menggunakan konsol untuk mengedit tanda yang telah ditambahkan ke sumber daya koneksi.

Untuk mengedit tag untuk koneksi

1. Masuk ke konsol . Dari panel navigasi, pilih Pengaturan.
2. Pada Pengaturan, pilih Koneksi. Pilih tab Koneksi.
3. Pilih koneksi yang ingin Anda edit. Halaman pengaturan koneksi ditampilkan.
4. Pada Tanda koneksi, pilih Edit. Halaman Tanda koneksi ditampilkan.
5. Di bidang Kunci dan Nilai, perbarui nilai di setiap bidang sesuai kebutuhan. Misalnya, untuk kunci **Project**, di Nilai, ubah **ProjectA** ke **ProjectB**.

6. Pilih Kirim.

Untuk mengedit tag untuk host

1. Masuk ke konsol . Dari panel navigasi, pilih Pengaturan.
2. Pada Pengaturan, pilih Koneksi. Pilih tab Host.
3. Pilih host yang ingin Anda edit. Halaman pengaturan host ditampilkan.
4. Pada Tanda host, pilih Edit. Halaman Tanda host ditampilkan.
5. Di bidang Kunci dan Nilai, perbarui nilai di setiap bidang sesuai kebutuhan. Misalnya, untuk kunci **Project**, di Nilai, ubah **ProjectA** ke **ProjectB**.
6. Pilih Kirim.

Hapus tanda dari sumber daya koneksi (konsol)

Anda dapat menggunakan konsol untuk menghapus tanda dari sumber daya koneksi. Saat Anda menghapus tanda dari sumber daya yang terkait, tanda akan dihapus.

Untuk menghapus tag untuk koneksi

1. Masuk ke konsol . Dari panel navigasi, pilih Pengaturan.
2. Pada Pengaturan, pilih Koneksi. Pilih tab Koneksi.
3. Pilih koneksi yang ingin Anda edit. Halaman pengaturan koneksi ditampilkan.
4. Pada Tanda koneksi, pilih Edit. Halaman Tanda koneksi ditampilkan.
5. Di samping kunci dan nilai untuk setiap tanda yang ingin Anda hapus, pilih Hapus tanda.
6. Pilih Kirim.

Untuk menghapus tag untuk host

1. Masuk ke konsol . Dari panel navigasi, pilih Pengaturan.
2. Pada Pengaturan, pilih Koneksi. Pilih tab Host.
3. Pilih host yang ingin Anda edit. Halaman pengaturan host ditampilkan.
4. Pada Tanda host, pilih Edit. Halaman Tanda host ditampilkan.
5. Di samping kunci dan nilai untuk setiap tanda yang ingin Anda hapus, pilih Hapus tanda.
6. Pilih Kirim.

Tanda sumber daya (CLI)

Anda dapat menggunakan CLI untuk melihat, menambah, memperbarui, atau menghapus tanda pada sumber daya koneksi.

Topik

- [Menambahkan tanda ke sumber daya koneksi \(CLI\)](#)
- [Melihat tanda untuk sumber daya koneksi \(CLI\)](#)
- [Edit tanda untuk sumber daya koneksi \(CLI\)](#)
- [Hapus tanda dari sumber daya koneksi \(CLI\)](#)

Menambahkan tanda ke sumber daya koneksi (CLI)

Anda dapat menggunakan AWS CLI untuk menandai sumber daya dalam koneksi.

Pada terminal atau baris perintah, jalankan perintah `tag-resource`, tentukan Amazon Resource Name (ARN) dari sumber daya tempat Anda ingin menambahkan tanda serta kunci dan nilai dari tanda yang ingin Anda tambahkan. Anda dapat menambahkan lebih dari satu tanda.

Untuk menambahkan tag untuk koneksi

1. Dapatkan ARN untuk sumber daya Anda. Gunakan perintah `list-connections` yang ditampilkan di [Daftar koneksi](#) untuk mendapatkan ARN koneksi.
2. Di terminal atau pada baris perintah, jalankan perintah `tag-resource`.

Misalnya, gunakan perintah berikut untuk menandai koneksi dengan dua tag, kunci tag bernama *Project* dengan nilai tag dari *ProjectA*, dan kunci tag bernama *ReadOnly* dengan nilai tag dari *true*.

```
aws codestar-connections tag-resource --resource-arn arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --tags Key=Project,Value=ProjectA Key=IscontainerBased,Value=true
```

Jika berhasil, perintah ini tidak mengembalikan apa pun.

Untuk menambahkan tag untuk host

1. Dapatkan ARN untuk sumber daya Anda. Gunakan perintah `list-hosts` yang ditampilkan di [Daftar host](#) untuk mendapatkan ARN host.
2. Di terminal atau pada baris perintah, jalankan perintah `tag-resource`.

Misalnya, gunakan perintah berikut untuk menandai host dengan dua tag, kunci tag bernama *Project* dengan nilai tag dari *ProjectA*, dan kunci tag bernama *IscontainerBased* dengan nilai tag dari *true*.

```
aws codestar-connections tag-resource --resource-arn arn:aws:codestar-connections:us-west-2:account_id:host/My-Host-28aef605 --tags Key=Project,Value=ProjectA Key=IscontainerBased,Value=true
```

Jika berhasil, perintah ini tidak mengembalikan apa pun.

Melihat tanda untuk sumber daya koneksi (CLI)

Anda dapat menggunakan AWS CLI untuk melihat AWS tag untuk sumber daya koneksi. Jika tidak ada tanda yang telah ditambahkan, daftar yang dikembalikan kosong. Gunakan perintah `list-tags-for-resource` untuk melihat tanda yang telah ditambahkan ke koneksi atau host.

Untuk melihat tag untuk koneksi

1. Dapatkan ARN untuk sumber daya Anda. Gunakan perintah `list-connections` yang ditampilkan di [Daftar koneksi](#) untuk mendapatkan ARN koneksi.
2. Di terminal atau pada baris perintah, jalankan perintah `list-tags-for-resource`. Misalnya, gunakan perintah berikut untuk melihat daftar kunci tanda dan nilai tanda untuk koneksi.

```
aws codestar-connections list-tags-for-resource --resource-arn arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Perintah ini mengembalikan tanda yang terkait dengan sumber daya. Contoh ini menunjukkan dua pasangan nilai kunci yang dikembalikan untuk koneksi.

```
{
  "Tags": [
    {
      "Key": "Project",
```

```
        "Value": "ProjectA"
      },
      {
        "Key": "ReadOnly",
        "Value": "true"
      }
    ]
  }
}
```

Untuk melihat tag untuk host

1. Dapatkan ARN untuk sumber daya Anda. Gunakan perintah `list-hosts` yang ditampilkan di [Daftar host](#) untuk mendapatkan ARN host.
2. Di terminal atau pada baris perintah, jalankan perintah `list-tags-for-resource`. Misalnya, gunakan perintah berikut untuk melihat daftar kunci tanda dan nilai tanda untuk host.

```
aws codestar-connections list-tags-for-resource --resource-arn arn:aws:codestar-connections:us-west-2:account_id:host/My-Host-28aef605
```

Perintah ini mengembalikan tanda yang terkait dengan sumber daya. Contoh ini menunjukkan dua pasangan nilai kunci yang dikembalikan untuk host.

```
{
  "Tags": [
    {
      "Key": "IscontainerBased",
      "Value": "true"
    },
    {
      "Key": "Project",
      "Value": "ProjectA"
    }
  ]
}
```

Edit tanda untuk sumber daya koneksi (CLI)

Anda dapat menggunakan AWS CLI untuk mengedit tag untuk sumber daya. Anda dapat mengubah nilai untuk kunci yang ada atau menambahkan kunci lain.

Pada terminal atau baris perintah, jalankan perintah `tag-resource`, tentukan ARN sumber daya tempat Anda ingin memperbarui tanda dan menentukan kunci tanda dan nilai tanda yang akan diperbarui.

Ketika Anda mengedit tanda, kunci tanda apa pun yang tidak ditentukan akan dipertahankan, sementara apa pun dengan kunci yang sama tetapi memiliki nilai baru akan diperbarui. Kunci baru yang ditambahkan dengan perintah edit ditambahkan sebagai pasangan nilai kunci baru.

Untuk mengedit tag untuk koneksi

1. Dapatkan ARN untuk sumber daya Anda. Gunakan perintah `list-connections` yang ditampilkan di [Daftar koneksi](#) untuk mendapatkan ARN koneksi.
2. Di terminal atau pada baris perintah, jalankan perintah `tag-resource`.

Dalam contoh ini, nilai untuk kunci `Project` diubah menjadi `ProjectB`.

```
aws codestar-connections tag-resource --resource-arn arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --tags Key=Project,Value=ProjectB
```

Jika berhasil, perintah ini tidak mengembalikan apa pun. Untuk memverifikasi tanda yang terkait dengan koneksi, jalankan perintah `list-tags-for-resource`.

Untuk mengedit tag untuk host

1. Dapatkan ARN untuk sumber daya Anda. Gunakan perintah `list-hosts` yang ditampilkan di [Daftar host](#) untuk mendapatkan ARN host.
2. Di terminal atau pada baris perintah, jalankan perintah `tag-resource`.

Dalam contoh ini, nilai untuk kunci `Project` diubah menjadi `ProjectB`.

```
aws codestar-connections tag-resource --resource-arn arn:aws:codestar-connections:us-west-2:account_id:host/My-Host-28aef605 --tags Key=Project,Value=ProjectB
```

Jika berhasil, perintah ini tidak mengembalikan apa pun. Untuk memverifikasi tanda yang terkait dengan host, jalankan perintah `list-tags-for-resource`.

Hapus tanda dari sumber daya koneksi (CLI)

Ikuti langkah-langkah ini untuk menggunakan AWS CLI untuk menghapus tag dari sumber daya. Saat Anda menghapus tanda dari sumber daya yang terkait, tanda akan dihapus.

Note

Jika Anda menghapus sumber daya koneksi, semua pengaitan tanda akan dihapus dari sumber daya yang dihapus. Anda tidak perlu menghapus tanda sebelum Anda menghapus sumber daya koneksi.

Pada terminal atau baris perintah, jalankan perintah `untag-resource`, tentukan ARN dari sumber daya tempat Anda ingin menghapus tanda serta kunci tanda dari tanda yang ingin Anda hapus. Misalnya, untuk menghapus beberapa tag pada koneksi dengan tombol tag *Project* dan *ReadOnly*, gunakan perintah berikut.

```
aws codestar-connections untag-resource --resource-arn arn:aws:codestar-connections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f --tag-keys Project ReadOnly
```

Jika berhasil, perintah ini tidak mengembalikan apa pun. Untuk memverifikasi tanda yang terkait dengan sumber daya, jalankan perintah `list-tags-for-resource`. Output menunjukkan bahwa semua tanda telah dihapus.

```
{  
  "Tags": []  
}
```

Melihat detail koneksi

Anda dapat menggunakan konsol Alat Pengembang atau `get-connection` perintah di AWS Command Line Interface (AWS CLI) untuk melihat detail sambungan. Untuk menggunakan AWS CLI, Anda harus sudah menginstal versi terbaru AWS CLI atau diperbarui ke versi saat ini. Untuk informasi selengkapnya, lihat [Menginstal AWS CLI](#) dalam AWS Command Line Interface Panduan Penggunaan.

Untuk melihat koneksi (konsol)

1. Buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan > Koneksi.
3. Pilih tombol di samping koneksi yang ingin Anda lihat, lalu pilih Lihat detail.
4. Informasi berikut muncul untuk koneksi Anda:
 - Nama koneksi.
 - Jenis penyedia untuk koneksi Anda.
 - Status koneksi.
 - ARN koneksi.
 - Jika koneksi dibuat untuk penyedia yang diinstal, seperti GitHub Enterprise Server, informasi host yang terkait dengan koneksi.
 - Jika koneksi dibuat untuk penyedia yang diinstal, seperti GitHub Enterprise Server, informasi titik akhir yang terkait dengan host untuk koneksi.
5. Jika koneksi dalam status Tertunda, untuk menyelesaikan koneksi, pilih Perbarui koneksi tertunda. Untuk informasi selengkapnya, lihat [Memperbarui koneksi yang tertunda](#).

Untuk melihat koneksi (CLI)

- Di terminal atau baris perintah, jalankan perintah `get-connection`. Misalnya, gunakan perintah berikut ini untuk melihat detail koneksi dengan nilai ARN `arn:aws:codeconnections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f`.

```
aws codeconnections get-connection --connection-arn arn:aws:codeconnections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Jika berhasil, perintah ini mengembalikan detail koneksi.

Contoh output untuk koneksi Bitbucket:

```
{
  "Connection": {
    "ConnectionName": "MyConnection",
```

```

    "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/
cdacd948-EXAMPLE",
    "ProviderType": "Bitbucket",
    "OwnerAccountId": "account_id",
    "ConnectionStatus": "AVAILABLE"
  }
}

```

Contoh output untuk GitHub koneksi:

```

{
  "Connection": {
    "ConnectionName": "MyGitHubConnection",
    "ConnectionArn": "arn:aws:codeconnections:us-west-2:account_id:connection/
ebcd4a13-EXAMPLE",
    "ProviderType": "GitHub",
    "OwnerAccountId": "account_id",
    "ConnectionStatus": "AVAILABLE"
  }
}

```

Contoh output untuk koneksi GitHub Enterprise Server:

```

{
  "Connection": {
    "ConnectionName": "MyConnection",
    "ConnectionArn": "arn:aws:codeconnections:us-
west-2:account_id:connection/2d178fb9-EXAMPLE",
    "ProviderType": "GitHubEnterpriseServer",
    "OwnerAccountId": "account_id",
    "ConnectionStatus": "PENDING",
    "HostArn": "arn:aws:codeconnections:us-west-2:account_id:host/sdfsdf-
EXAMPLE"
  }
}

```

Berbagi koneksi dengan Akun AWS

Anda dapat menggunakan berbagi sumber daya AWS RAM untuk berbagi koneksi yang ada dengan orang lain Akun AWS atau dengan akun di organisasi Anda. Anda dapat menggunakan koneksi

bersama dengan sumber daya AWS yang Anda kelola untuk koneksi sumber pihak ketiga, seperti di CodePipeline.

Important

Berbagi koneksi tidak didukung untuk `codestar-connections` sumber daya. Ini hanya didukung untuk `codeconnections` sumber daya.

Sebelum Anda memulai:

- Anda harus sudah membuat koneksi dengan Anda Akun AWS.
- Anda harus mengaktifkan berbagi sumber daya.
- Anda harus memiliki izin yang diperlukan yang dikonfigurasi. Untuk informasi selengkapnya, lihat [Izin yang didukung untuk berbagi koneksi](#).

Note

Untuk berbagi koneksi, Anda harus menjadi pemilik organisasi atau pemilik repositori jika tidak di bawah organisasi. Akun yang Anda bagikan juga memerlukan izin ke repositori.

Topik

- [Bagikan koneksi \(konsol\)](#)
- [Bagikan koneksi \(CLI\)](#)
- [Lihat koneksi bersama \(konsol\)](#)
- [Lihat koneksi bersama \(CLI\)](#)

Bagikan koneksi (konsol)

Anda dapat menggunakan konsol untuk membuat sumber daya koneksi bersama.

1. Masuk ke Konsol Manajemen AWS.

Pilih Buat berbagi sumber daya di halaman [Dibagikan oleh saya: Sumber daya bersama](#) di AWS RAM konsol.

2. Karena pembagian AWS RAM sumber daya ada di Wilayah AWS tertentu, pilih Wilayah AWS yang sesuai dari daftar tarik-turun di sudut kanan atas konsol. Untuk membuat pembagian sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke AS Timur (Virginia Utara),

Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).

3. Pada halaman pembuatan, di Nama, masukkan nama untuk berbagi sumber daya Anda. Di bawah Sumber Daya, pilih Koneksi Kode.

Resource Access Manager > Shared by me: Resource shares > Create resource share

Step 4

Grant access to principals

Step 4

Review and create

Name
Provide a descriptive name for the resource share.

Add resource share name

Resources - optional
Choose the resources to add to the resource share

Select resource type

Filter by text

code

Code Connections

CodeBuild Projects

CodeBuild Report Groups

Code Connections

No resources to display
Select a resource type filter

Selected resources (0)

Filter by text

Resource ID

Resource type

No resources selected

4. Pilih sumber daya koneksi Anda dan tetapkan prinsipal dengan siapa Anda ingin berbagi.
5. Pilih Buat.

Bagikan koneksi (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk berbagi koneksi yang ada dengan akun lain dan melihat koneksi yang Anda miliki atau telah berbagi dengan Anda.

Untuk melakukan ini, gunakan `accept-resource-share-invitation` perintah `create-resource-share` dan untuk AWS RAM.

Untuk berbagi koneksi

1. Masuk dengan akun yang akan berbagi koneksi.

2. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-resource-share` perintah, menentukan, `--name`, `--resource-arns`, dan `--principals` untuk berbagi koneksi Anda. Dalam contoh ini, namanya `my-shared-resource` dan nama koneksi yang ditentukan ada `MyConnection` di sumber daya ARN. `Diprincipals`, berikan akun tujuan atau akun yang Anda bagikan.

```
aws ram create-resource-share --name my-shared-resource --resource-arns connection_ARN --principals destination_account
```

Jika berhasil, perintah ini mengembalikan informasi ARN koneksi seperti berikut ini.

```
{
  "resourceShare": {
    "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-share/4476c27d-8feb-4b21-afe9-7de23EXAMPLE",
    "name": "MyNewResourceShare",
    "owningAccountId": "111111111111",
    "allowExternalPrincipals": true,
    "status": "ACTIVE",
    "creationTime": 1634586271.302,
    "lastUpdatedTime": 1634586271.302
  }
}
```

3. Permintaan untuk berbagi dapat diterima sebagaimana dirinci dalam prosedur selanjutnya.

Untuk mengautentikasi dan menerima pembagian koneksi dengan akun tujuan

Prosedur berikut bersifat opsional untuk akun tujuan yang dimiliki oleh organisasi yang sama dan mengaktifkan pembagian sumber daya di Organizations.

1. Masuk dengan akun tujuan yang akan menerima undangan.
2. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `get-resource-share-invitations` perintah.

```
aws ram get-resource-share-invitations
```

Tangkap ARN undangan berbagi sumber daya untuk langkah selanjutnya.

3. Jalankan `accept-resource-share-invitation` perintah, tentukan. `--resource-share-invitation-arn`

```
aws ram accept-resource-share-invitation --resource-share-invitation-arn invitation_ARN
```

Jika berhasil, perintah ini mengembalikan output berikut.

```
{
  "resourceShareInvitation": {
    "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111111111111:resource-share-invitation/1e3477be-4a95-46b4-bbe0-c4001EXAMPLE",
    "resourceShareName": "MyResourceShare",
    "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE",
    "senderAccountId": "111111111111",
    "receiverAccountId": "222222222222",
    "invitationTimestamp": "2021-09-22T15:07:35.620000-07:00",
    "status": "ACCEPTED"
  }
}
```

Lihat koneksi bersama (konsol)

Anda dapat menggunakan konsol untuk melihat sumber daya koneksi bersama.

1. Masuk ke Konsol Manajemen AWS.

Buka halaman [Shared by me: Shared resources](#) di AWS RAM console.

2. Karena pembagian sumber daya AWS RAM ada di Wilayah AWS tertentu, pilih Wilayah AWS yang sesuai dari daftar tarik-turun di sudut kanan atas konsol. Untuk melihat pembagian sumber daya yang berisi sumber daya global, Anda harus menetapkan Wilayah AWS ke AS Timur (Virginia Utara),

Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).

3. Untuk setiap sumber daya bersama, informasi berikut tersedia:

- ID Sumber Daya — ID dari sumber daya. Pilih ID sumber daya untuk membuka tab browser baru untuk melihat sumber daya di konsol layanan aslinya.
- Jenis sumber daya — Jenis sumber daya.
- Tanggal berbagi terakhir — Tanggal di mana sumber daya terakhir dibagikan.
- Pembagian sumber daya — Jumlah pembagian sumber daya yang mencakup sumber daya. Untuk melihat daftar pembagian sumber daya, pilih nomornya.
- Prinsipal — Jumlah kepala sekolah yang dapat mengakses sumber daya. Pilih nilai untuk melihat prinsipal.

Lihat koneksi bersama (CLI)

Anda dapat menggunakan AWS CLI untuk melihat koneksi yang Anda miliki atau telah berbagi dengan Anda.

Untuk melakukannya, gunakan perintah `get-resource-shares`.

Untuk melihat koneksi bersama

- Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `get-resource-shares` perintah.

```
aws iam get-resource-shares
```

Output mengembalikan daftar pembagian sumber daya untuk akun Anda.

Bekerja dengan host

Untuk membuat sambungan ke jenis penyedia yang diinstal, seperti GitHub Enterprise Server, Anda terlebih dahulu membuat host menggunakan Konsol Manajemen AWS. Host adalah sumber daya yang Anda buat untuk mewakili infrastruktur tempat penyedia Anda diinstal. Kemudian Anda membuat koneksi menggunakan host tersebut. Untuk informasi lebih lanjut, lihat [Bekerja dengan koneksi](#).

Misalnya, Anda membuat host untuk koneksi Anda sehingga aplikasi pihak ketiga untuk penyedia Anda dapat didaftarkan untuk mewakili infrastruktur Anda. Anda membuat satu host untuk jenis penyedia, dan kemudian semua koneksi Anda ke jenis penyedia tersebut menggunakan host tersebut.

Saat Anda menggunakan konsol untuk membuat sambungan ke jenis penyedia yang diinstal, seperti GitHub Enterprise Server, konsol akan membuat sumber daya host untuk Anda.

Topik

- [Membuat host](#)
- [Menyiapkan host yang tertunda](#)
- [Daftar host](#)
- [Mengedit host](#)
- [Menghapus host](#)
- [Melihat detail host](#)

Membuat host

Anda dapat menggunakan Konsol Manajemen AWS atau AWS Command Line Interface (AWS CLI) untuk membuat koneksi ke repositori kode pihak ketiga yang diinstal pada infrastruktur Anda. Misalnya, Anda mungkin menjalankan GitHub Enterprise Server sebagai mesin virtual pada instans Amazon EC2. Sebelum Anda membuat koneksi ke GitHub Enterprise Server, Anda membuat host untuk digunakan untuk koneksi.

Untuk ikhtisar alur kerja pembuatan host untuk penyedia yang diinstal, lihat [Alur kerja untuk membuat atau memperbarui host](#).

Sebelum Anda memulai:

- (Opsional) Jika Anda ingin membuat host Anda dengan VPC, Anda harus sudah membuat jaringan atau virtual private cloud (VPC).
- Anda harus sudah membuat instans Anda dan, jika Anda berencana untuk terhubung dengan VPC Anda, luncurkan host Anda ke VPC Anda.

Note

Setiap VPC hanya dapat dikaitkan dengan satu host pada satu waktu.

Anda dapat mengonfigurasi host Anda secara opsional dengan VPC. Untuk informasi selengkapnya tentang konfigurasi jaringan dan VPC untuk sumber daya host Anda, lihat prasyarat VPC di dan.

(Opsional) Prasyarat: Konfigurasi VPC Jaringan atau Amazon untuk koneksi Anda Pemecahan masalah konfigurasi VPC untuk host Anda

Untuk menggunakan konsol untuk membuat host dan koneksi ke GitHub Enterprise Server, lihat [Buat koneksi GitHub Enterprise Server Anda \(konsol\)](#). Konsol membuat host Anda untuk Anda.

Untuk menggunakan konsol untuk membuat host dan koneksi ke GitLab kelola sendiri, lihat [Buat koneksi ke GitLab self-managed](#). Konsol membuat host Anda untuk Anda.

(Opsional) Prasyarat: Konfigurasi VPC Jaringan atau Amazon untuk koneksi Anda

Jika infrastruktur Anda dikonfigurasi dengan koneksi jaringan, Anda dapat melewati bagian ini.

Jika host Anda hanya dapat diakses di VPC, ikuti persyaratan VPC ini sebelum melanjutkan.

Persyaratan VPC

Anda dapat memilih untuk membuat host Anda dengan VPC. Berikut ini adalah persyaratan VPC umum, tergantung pada VPC yang telah Anda atur untuk instalasi Anda.

- Anda dapat mengonfigurasi VPC publik dengan subnet publik dan privat. Anda dapat menggunakan VPC default untuk Anda Akun AWS jika Anda tidak memiliki blok CIDR atau subnet pilihan.
- Jika Anda memiliki VPC pribadi yang dikonfigurasi, dan Anda telah mengonfigurasi instance Server GitHub Perusahaan Anda untuk melakukan validasi TLS menggunakan otoritas sertifikat non-publik, Anda harus memberikan sertifikat TLS untuk sumber daya host Anda.
- Saat koneksi membuat host Anda, titik akhir VPC (PrivateLink) untuk webhook dibuat untuk Anda. Untuk informasi selengkapnya, lihat [AWS CodeConnections dan antarmuka titik akhir VPC \(AWS PrivateLink\)](#).
- Konfigurasi grup keamanan:
 - Grup keamanan yang digunakan selama pembuatan host memerlukan aturan masuk dan keluar yang memungkinkan antarmuka jaringan terhubung ke instance Server GitHub Perusahaan Anda
 - Grup keamanan yang dilampirkan ke instance GitHub Enterprise Server Anda (bukan bagian dari penyiapan host) memerlukan akses masuk dan keluar dari antarmuka jaringan yang dibuat oleh koneksi.
- Subnet VPC Anda harus berada di Availability Zone yang berbeda di Wilayah Anda. Availability Zone adalah lokasi berbeda yang diisolasi dari kegagalan di Availability Zone lainnya. Setiap

subnet harus berada sepenuhnya dalam satu Availability Zone dan tidak dapat merentangkan zona.

Untuk informasi selengkapnya tentang bekerja dengan VPCs dan subnet, lihat Ukuran [VPC dan Subnet untuk IPv4 di Panduan](#) Pengguna Amazon VPC.

Informasi VPC yang Anda berikan untuk penyiapan host

Ketika Anda membuat sumber daya host Anda untuk koneksi Anda pada langkah berikutnya, Anda harus memberikan hal berikut:

- ID VPC: ID VPC untuk server tempat instans Server GitHub Perusahaan Anda diinstal atau VPC yang memiliki akses ke instans Server GitHub Perusahaan yang diinstal melalui VPN atau Direct Connect.
- Subnet ID atau IDs: ID subnet untuk server tempat instans Server GitHub Enterprise Anda diinstal atau subnet dengan akses ke instance GitHub Enterprise Server yang diinstal melalui VPN atau Direct Connect.
- Grup atau grup keamanan: Grup keamanan untuk server tempat instans Server GitHub Perusahaan Anda diinstal atau grup keamanan dengan akses ke instans Server GitHub Perusahaan yang diinstal melalui VPN atau Direct Connect.
- Titik akhir: Siapkan titik akhir server Anda dan lanjutkan ke langkah berikutnya.

Untuk informasi lebih lanjut, termasuk pemecahan masalah koneksi VPC atau host, lihat [Pemecahan masalah konfigurasi VPC untuk host Anda](#).

Persyaratan izin

Sebagai bagian dari proses pembuatan host, AWS CodeConnections buat sumber daya jaringan atas nama Anda untuk memfasilitasi konektivitas VPC. Ini termasuk antarmuka jaringan AWS CodeConnections untuk kueri data dari host Anda, dan titik akhir VPC atau host PrivateLink untuk mengirim data peristiwa melalui webhook ke koneksi. Untuk dapat membuat sumber daya jaringan ini, pastikan bahwa peran yang digunakan untuk membuat host memiliki izin berikut:

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptions
ec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
```

```
ec2:DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2>DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

Untuk informasi selengkapnya tentang pemecahan masalah izin atau koneksi host di VPC, lihat [Pemecahan masalah konfigurasi VPC untuk host Anda](#).

Untuk informasi selengkapnya tentang VPC endpoint webhook, lihat [AWS CodeConnections dan antarmuka titik akhir VPC \(AWS PrivateLink\)](#).

Topik

- [Membuat host untuk koneksi \(konsol\)](#)
- [Buat host untuk koneksi \(CLI\)](#)

Membuat host untuk koneksi (konsol)

Untuk koneksi untuk instalasi, seperti dengan GitHub Enterprise Server atau dengan GitLab dikelola sendiri, Anda menggunakan host untuk mewakili titik akhir infrastruktur tempat penyedia pihak ketiga Anda diinstal.

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan codeconnections ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Untuk mempelajari tentang pertimbangan menyiapkan host di VPC, lihat [Buat koneksi ke GitLab self-managed](#).

Untuk menggunakan konsol untuk membuat host dan koneksi ke GitHub Enterprise Server, lihat [Buat koneksi GitHub Enterprise Server Anda \(konsol\)](#). Konsol membuat host Anda untuk Anda.

Untuk menggunakan konsol untuk membuat host dan koneksi ke GitLab kelola sendiri, lihat [Buat koneksi ke GitLab self-managed](#). Konsol membuat host Anda untuk Anda.

Note

Anda hanya membuat host satu kali per Server GitHub Perusahaan atau akun yang GitLab dikelola sendiri. Semua koneksi Anda ke Server GitHub Perusahaan tertentu atau akun yang GitLab dikelola sendiri akan menggunakan host yang sama.

Buat host untuk koneksi (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk membuat host untuk koneksi terinstal.

Note

Anda hanya membuat host satu kali per akun GitHub Enterprise Server. Semua koneksi Anda ke akun GitHub Enterprise Server tertentu akan menggunakan host yang sama.

Anda menggunakan host untuk mewakili titik akhir infrastruktur tempat penyedia pihak ketiga Anda diinstal. Untuk membuat sebuah host dengan CLI, Anda menggunakan perintah `create-host`. Setelah Anda selesai membuat host, host dalam status Tertunda. Anda kemudian mengatur host untuk memindahkannya ke status Tersedia. Setelah host tersedia, Anda menyelesaikan langkah-langkah untuk membuat koneksi.

Important

Host yang dibuat melalui status AWS CLI berada dalam Pending status secara default. Setelah Anda membuat host dengan CLI, gunakan konsol untuk mengatur host untuk membuat statusnya Available.

Untuk menggunakan konsol untuk membuat host dan koneksi ke GitHub Enterprise Server, lihat [Buat koneksi GitHub Enterprise Server Anda \(konsol\)](#). Konsol membuat host Anda untuk Anda.

Untuk menggunakan konsol untuk membuat host dan koneksi ke GitLab kelola sendiri, lihat [Buat koneksi ke GitLab self-managed](#). Konsol membuat host Anda untuk Anda.

Menyiapkan host yang tertunda

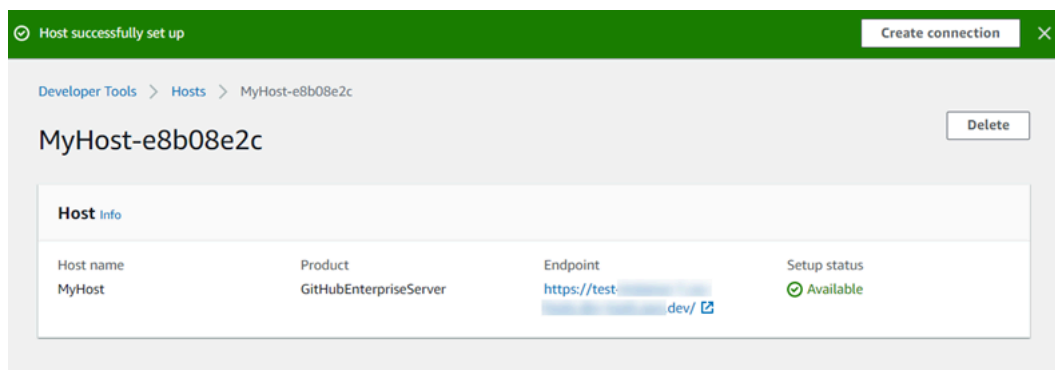
Host yang dibuat melalui AWS Command Line Interface (AWS CLI) atau SDK dalam Pending status secara default. Setelah Anda membuat koneksi dengan konsol AWS CLI, atau SDK, gunakan konsol untuk mengatur host untuk membuat statusnya Available.

Anda harus sudah membuat host. Untuk informasi selengkapnya, lihat [Membuat host](#).

Untuk menyiapkan host yang tertunda

Setelah host Anda dibuat, itu dalam status Tertunda. Untuk memindahkan host dari Tertunda ke Tersedia, selesaikan langkah-langkah ini. Proses ini melakukan jabat tangan dengan penyedia pihak ketiga untuk mendaftarkan aplikasi AWS koneksi di host.

1. Setelah host Anda mencapai status Tertunda di konsol Alat AWS Pengembang, pilih Siapkan host.
2. Jika Anda membuat host untuk GitLab dikelola sendiri, halaman Siapkan akan ditampilkan. Di Berikan token akses pribadi, berikan GitLab PAT Anda dengan izin cakupan bawah yang diikuti saja: api.
3. Pada halaman login penyedia yang diinstal pihak ketiga, seperti halaman login GitHub Enterprise Server, masuk dengan kredensi akun Anda jika diminta.
4. Pada halaman penginstalan GitHub aplikasi, di Nama aplikasi, masukkan nama untuk aplikasi yang ingin Anda instal untuk host Anda. Pilih Buat GitHub Aplikasi.
5. Setelah host Anda berhasil terdaftar, halaman detail host muncul dan menunjukkan bahwa status host Tersedia.



6. Anda dapat melanjutkan dengan membuat koneksi Anda setelah host tersedia. Pada banner sukses, pilih Buat koneksi. Selesaikan langkah-langkah dalam [Membuat koneksi](#).

Daftar host

Anda dapat menggunakan konsol Alat Pengembang atau `list-connections` perintah di AWS Command Line Interface (AWS CLI) untuk melihat daftar koneksi di akun Anda.

Daftar host (konsol)

Untuk daftar host

1. Buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih tab Host. Lihat nama, status, dan ARN untuk host Anda.

Daftar host (CLI)

Anda dapat menggunakan daftar host Anda untuk koneksi penyedia pihak ketiga yang diinstal. AWS CLI

Untuk melakukannya, gunakan perintah `list-hosts`.

Untuk daftar host

- Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows), dan gunakan AWS CLI untuk menjalankan perintah. `list-hosts`

```
aws codeconnections list-hosts
```

Perintah ini mengembalikan output berikut.

```
{
  "Hosts": [
    {
      "Name": "My-Host",
      "HostArn": "arn:aws:codeconnections:us-west-2:account_id:host/My-Host-28aef605",
      "ProviderType": "GitHubEnterpriseServer",
      "ProviderEndpoint": "https://my-instance.test.dev",
      "Status": "AVAILABLE"
    }
  ]
}
```

Mengedit host

Anda dapat mengedit pengaturan host untuk host dalam status Pending. Anda dapat mengedit nama host, URL, atau konfigurasi VPC.

Anda tidak dapat menggunakan URL yang sama untuk lebih dari satu host.

Note

Untuk mempelajari tentang pertimbangan menyiapkan host di VPC, lihat [\(Opsional\) Prasyarat: Konfigurasi VPC Jaringan atau Amazon untuk koneksi Anda](#).

Untuk mengedit host

1. Buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan > Koneksi.
3. Pilih tab Host.

Host yang terkait dengan AWS akun Anda dan dibuat di AWS Wilayah yang dipilih ditampilkan.

4. Untuk mengedit nama host, masukkan nilai baru di Nama.
5. Untuk mengedit titik akhir host, masukkan nilai baru di URL.
6. Untuk mengedit konfigurasi VPC host, masukkan nilai baru di ID VPC.
7. Pilih Edit host.
8. Pengaturan yang diperbarui akan ditampilkan. Pilih Menyiapkan host Tertunda.

Menghapus host

Anda dapat menggunakan konsol Alat Pengembang atau delete-host perintah di AWS Command Line Interface (AWS CLI) untuk menghapus host.

Topik

- [Hapus host \(konsol\)](#)
- [Menghapus host \(CLI\)](#)

Hapus host (konsol)

Untuk menghapus host

1. Buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih tab Host. Di Nama, pilih nama host yang ingin Anda hapus.
3. Pilih Hapus.
4. Masukkan **delete** di bidang untuk mengonfirmasi, lalu pilih Hapus.

Important

Tindakan ini tidak dapat dibatalkan.

Menghapus host (CLI)

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menghapus host.

Untuk melakukannya, gunakan perintah delete-host.

Important

Sebelum Anda dapat menghapus host, Anda harus menghapus semua koneksi yang terkait dengan host.

Setelah Anda menjalankan perintah tersebut, host dihapus. Tidak ada kotak dialog konfirmasi yang ditampilkan.

Untuk menghapus host

- Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan tombol AWS CLI untuk menjalankan delete-host perintah, dengan menentukan Amazon Resource Name (ARN) dari host yang ingin Anda hapus.

```
aws codeconnections delete-host --host-arn "arn:aws:codeconnections:us-west-2:account_id:host/My-Host-28aef605"
```

Perintah ini tidak mengembalikan apa pun.

Melihat detail host

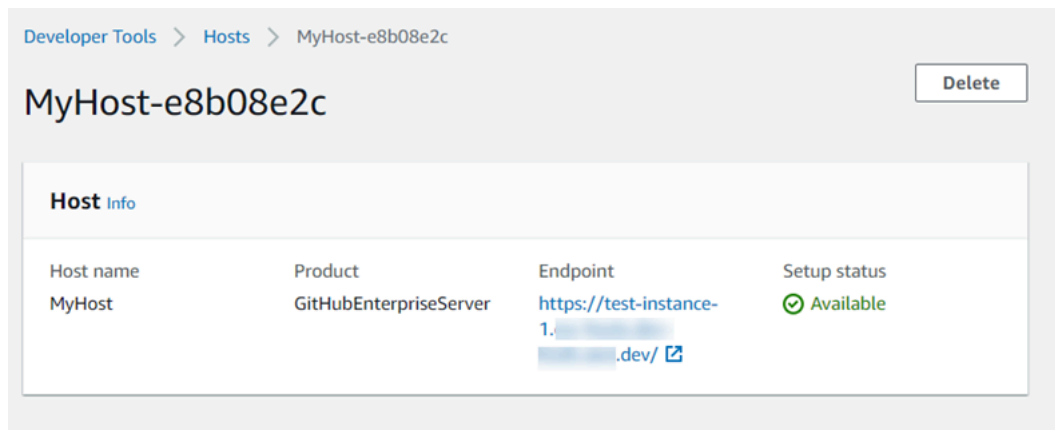
Anda dapat menggunakan konsol Alat Developer atau perintah `get-host` di AWS Command Line Interface (AWS CLI) untuk melihat detail host.

Untuk melihat detail host (konsol)

1. Masuk ke Konsol Manajemen AWS dan buka konsol Alat Pengembang di <https://console.aws.amazon.com/codesuite/settings/connections>.
2. Pilih Pengaturan > Koneksi, dan kemudian pilih tab Host.
3. Pilih tombol di samping host yang ingin Anda lihat, lalu pilih Lihat detail.
4. Informasi berikut muncul untuk host Anda:
 - Nama host.
 - Jenis penyedia untuk koneksi Anda.
 - Titik akhir infrastruktur tempat penyedia Anda diinstal.
 - Status penyiapan untuk host Anda. Sebuah host siap untuk koneksi berada dalam status Tersedia. Jika host Anda telah dibuat tetapi penyiapannya belum selesai, host tersebut mungkin berada dalam status yang berbeda.

Status berikut tersedia:

- TERTUNDA - Host telah menyelesaikan pembuatan dan siap untuk memulai penyiapan dengan mendaftarkan aplikasi penyedia di host.
- TERSEDIA - Host telah menyelesaikan pembuatan serta penyiapan dan tersedia untuk digunakan dengan koneksi.
- KESALAHAN - Terjadi kesalahan selama pembuatan atau pendaftaran host.
- VPC_CONFIG_VPC_INITIALIZING - Konfigurasi VPC untuk host sedang dibuat.
- VPC_CONFIG_VPC_FAILED_INITIALIZATION - Konfigurasi VPC untuk host yang ditemui dan kesalahan serta gagal.
- VPC_CONFIG_VPC_AVAILABLE - Konfigurasi VPC untuk host telah menyelesaikan penyiapan dan tersedia.
- VPC_CONFIG_VPC_DELETING - Konfigurasi VPC untuk host sedang dihapus.



- Untuk menghapus host, pilih Hapus.
- Jika host dalam status Tertunda, untuk menyelesaikan penyiapan, pilih Siapkan host. Untuk informasi selengkapnya, lihat [Menyiapkan host yang tertunda](#).

Untuk melihat detail host (CLI)

- Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows), dan gunakan AWS CLI untuk menjalankan get-host perintah, dengan menentukan Amazon Resource Name (ARN) dari host yang ingin Anda lihat detailnya.

```
aws codeconnections get-host --host-arn arn:aws:codeconnections:us-west-2:account_id:host/My-Host-28aef605
```

Perintah ini mengembalikan output berikut.

```
{
  "Name": "MyHost",
  "Status": "AVAILABLE",
  "ProviderType": "GitHubEnterpriseServer",
  "ProviderEndpoint": "https://test-instance-1.dev/"
}
```

Bekerja dengan konfigurasi sinkronisasi untuk repositori tertaut

Di AWS CodeConnections, Anda menggunakan koneksi untuk mengaitkan AWS sumber daya ke repositori pihak ketiga, seperti, Bitbucket Cloud GitHub, GitHub Enterprise Server, dan. GitLab

Menggunakan jenis CFN_STACK_SYNC sinkronisasi, Anda dapat membuat konfigurasi sinkronisasi, yang memungkinkan AWS untuk menyinkronkan konten dari repositori Git untuk memperbarui sumber daya tertentu AWS . CloudFormation terintegrasi dengan koneksi sehingga Anda dapat menggunakan sinkronisasi Git untuk mengelola template dan file parameter Anda dalam repositori tertaut yang Anda sinkronkan dengan.

Setelah membuat koneksi, Anda dapat menggunakan koneksi CLI atau CloudFormation konsol untuk membuat tautan repositori dan konfigurasi sinkronisasi.

- Tautan repositori: Tautan repositori menciptakan hubungan antara koneksi Anda dan repositori Git eksternal. Tautan repositori memungkinkan sinkronisasi Git untuk memantau dan menyinkronkan perubahan ke file dalam repositori Git tertentu.
- Konfigurasi sinkronisasi: Gunakan konfigurasi sinkronisasi untuk menyinkronkan konten dari repositori Git untuk memperbarui sumber daya tertentu AWS .

Untuk informasi lebih lanjut, lihat [Referensi API AWS CodeConnections](#) .

Untuk tutorial yang memandu Anda dalam membuat konfigurasi sinkronisasi untuk CloudFormation tumpukan menggunakan CloudFormation konsol, lihat [Bekerja dengan sinkronisasi CloudFormation Git](#) di Panduan CloudFormation Pengguna.

Topik

- [Bekerja dengan tautan repositori](#)
- [Bekerja dengan konfigurasi sinkronisasi](#)

Bekerja dengan tautan repositori

Tautan repositori menciptakan hubungan antara koneksi Anda dan repositori Git eksternal. Tautan repositori memungkinkan sinkronisasi Git untuk memantau dan menyinkronkan perubahan ke file dalam repositori Git tertentu ke tumpukan. CloudFormation

Untuk informasi selengkapnya tentang tautan repositori, lihat referensi [AWS CodeConnections API](#).

Topik

- [Buat tautan repositori](#)
- [Perbarui tautan repositori](#)
- [Daftar tautan repositori](#)

- [Hapus tautan repositori](#)
- [Lihat detail tautan repositori](#)

Buat tautan repositori

Anda dapat menggunakan `create-repository-link` perintah di AWS Command Line Interface (AWS CLI) untuk membuat tautan antara koneksi Anda dan repositori eksternal untuk disinkronkan.

Sebelum Anda dapat membuat tautan repositori, Anda harus sudah membuat repositori eksternal Anda dengan penyedia pihak ketiga Anda, seperti. GitHub

Untuk membuat link repositori

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `create-repository-link` perintah. Tentukan ARN dari koneksi terkait, ID pemilik, dan nama repositori.

```
aws codeconnections create-repository-link --connection-arn
arn:aws:codeconnections:us-east-1:account_id:connection/001f5be2-a661-46a4-
b96b-4d277cac8b6e --owner-id account_id --repository-name MyRepo
```

2. Perintah ini mengembalikan output berikut.

```
{
  "RepositoryLinkInfo": {
    "ConnectionArn": "arn:aws:codeconnections:us-east-1:account_id:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
    "OwnerId": "account_id",
    "ProviderType": "GitHub",
    "RepositoryLinkArn": "arn:aws:codeconnections:us-
east-1:account_id:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
    "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
    "RepositoryName": "MyRepo",
    "Tags": []
  }
}
```

Perbarui tautan repositori

Anda dapat menggunakan `update-repository-link` perintah di AWS Command Line Interface (AWS CLI) untuk memperbarui tautan repositori tertentu.

Anda dapat memperbarui informasi berikut untuk tautan repositori Anda:

- `--connection-arn`
- `--owner-id`
- `--repository-name`

Anda dapat memperbarui tautan repositori ketika Anda ingin mengubah koneksi yang terkait dengan repositori Anda. Untuk menggunakan koneksi yang berbeda, Anda perlu menentukan koneksi ARN. Untuk langkah-langkah untuk melihat ARN koneksi Anda, lihat [Melihat detail koneksi](#).

Untuk memperbarui tautan repositori

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `update-repository-link` perintah, menentukan nilai untuk memperbarui untuk link repositori. Misalnya, perintah berikut memperbarui koneksi yang terkait dengan ID tautan repositori. Ini menentukan ARN koneksi baru dengan `--connection` parameter.

```
aws codestar-connections update-repository-link --repository-link-id
6053346f-8a33-4edb-9397-10394b695173 --connection-arn arn:aws:codestar-
connections:us-east-1:account_id:connection/aEXAMPLE-f055-4843-adeb-4ceaefcb2167
```

2. Perintah ini mengembalikan output berikut.

```
{
  "RepositoryLinkInfo": {
    "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-f055-4843-adeb-4ceaefcb2167",
    "OwnerId": "owner_id",
    "ProviderType": "GitHub",
    "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/6053346f-8a33-4edb-9397-10394b695173",
    "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
    "RepositoryName": "MyRepo",
    "Tags": []
  }
}
```

```
}
```

Daftar tautan repositori

Anda dapat menggunakan `list-repository-links` perintah di AWS Command Line Interface (AWS CLI) untuk membuat daftar tautan repositori untuk akun Anda.

Untuk membuat daftar tautan repositori

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `list-repository-links` perintah.

```
aws codeconnections list-repository-links
```

2. Perintah ini mengembalikan output berikut.

```
{
  "RepositoryLinks": [
    {
      "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e",
      "OwnerId": "owner_id",
      "ProviderType": "GitHub",
      "RepositoryLinkArn": "arn:aws:codestar-connections:us-
east-1:account_id:repository-link/6053346f-8a33-4edb-9397-10394b695173",
      "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
      "RepositoryName": "MyRepo",
      "Tags": []
    }
  ]
}
```

Hapus tautan repositori

Anda dapat menggunakan `delete-repository-link` perintah di AWS Command Line Interface (AWS CLI) untuk menghapus tautan repositori.

Sebelum Anda dapat menghapus tautan repositori, Anda harus menghapus semua konfigurasi sinkronisasi yang terkait dengan tautan repositori.

⚠ Important

Setelah Anda menjalankan perintah, tautan repositori dihapus. Tidak ada kotak dialog konfirmasi yang ditampilkan. Anda dapat membuat tautan repositori baru, tetapi Nama Sumber Daya Amazon (ARN) tidak digunakan kembali.

Untuk menghapus tautan repositori

- Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `delete-repository-link` perintah, menentukan ID dari link repositori untuk menghapus.

```
aws codeconnections delete-repository-link --repository-link-id
6053346f-8a33-4edb-9397-10394b695173
```

Perintah ini tidak mengembalikan apa pun.

Lihat detail tautan repositori

Anda dapat menggunakan `get-repository-link` perintah di AWS Command Line Interface (AWS CLI) untuk melihat detail tentang link repositori.

Untuk melihat detail tautan repositori

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `get-repository-link` perintah, menentukan ID tautan repositori.

```
aws codestar-connections get-repository-link --repository-link-id
6053346f-8a33-4edb-9397-10394b695173
```

2. Perintah ini mengembalikan output berikut.

```
{
  "RepositoryLinkInfo": {
    "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
    "OwnerId": "owner_id",
    "ProviderType": "GitHub",
```

```
    "RepositoryLinkArn": "arn:aws:codestar-connections:us-  
east-1:account_id:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",  
    "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",  
    "RepositoryName": "MyRepo",  
    "Tags": []  
  }  
}
```

Bekerja dengan konfigurasi sinkronisasi

Konfigurasi sinkronisasi menciptakan hubungan antara repositori dan koneksi tertentu. Gunakan konfigurasi sinkronisasi untuk menyinkronkan konten dari repositori Git untuk memperbarui sumber daya tertentu AWS .

Untuk informasi selengkapnya tentang koneksi, lihat [referensi AWS CodeConnections API](#).

Topik

- [Buat konfigurasi sinkronisasi](#)
- [Perbarui konfigurasi sinkronisasi](#)
- [Konfigurasi sinkronisasi daftar](#)
- [Hapus konfigurasi sinkronisasi](#)
- [Lihat detail konfigurasi sinkronisasi](#)

Buat konfigurasi sinkronisasi

Anda dapat menggunakan create-repository-link perintah di AWS Command Line Interface (AWS CLI) untuk membuat tautan antara koneksi Anda dan repositori eksternal untuk disinkronkan.

Sebelum Anda dapat membuat konfigurasi sinkronisasi, Anda harus sudah membuat tautan repositori antara koneksi Anda dan repositori pihak ketiga Anda.

Untuk membuat konfigurasi sinkronisasi

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan create-repository-link perintah. Tentukan ARN dari koneksi terkait, ID pemilik, dan nama repositori. Perintah berikut membuat konfigurasi sinkronisasi dengan tipe sinkronisasi untuk sumber daya di CloudFormation. Ini juga menentukan cabang repositori

dan file konfigurasi di repositori. Dalam contoh ini, sumber daya adalah tumpukan bernama **mystack**.

```
aws codeconnections create-sync-configuration --branch main --config-file filename
--repository-link-id be8f2017-b016-4a77-87b4-608054f70e77 --resource-name mystack
--role-arn arn:aws:iam::account_id:role/myrole --sync-type CFN_STACK_SYNC
```

2. Perintah ini mengembalikan output berikut.

```
{
  "SyncConfiguration": {
    "Branch": "main",
    "ConfigFile": "filename",
    "OwnerId": "account_id",
    "ProviderType": "GitHub",
    "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
    "RepositoryName": "MyRepo",
    "ResourceName": "mystack",
    "RoleArn": "arn:aws:iam::account_id:role/myrole",
    "SyncType": "CFN_STACK_SYNC"
  }
}
```

Perbarui konfigurasi sinkronisasi

Anda dapat menggunakan `update-sync-configuration` perintah di AWS Command Line Interface (AWS CLI) untuk memperbarui konfigurasi sinkronisasi tertentu.

Anda dapat memperbarui informasi berikut untuk konfigurasi sinkronisasi Anda:

- `--branch`
- `--config-file`
- `--repository-link-id`
- `--resource-name`
- `--role-arn`

Untuk memperbarui konfigurasi sinkronisasi

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `update-sync-configuration` perintah, menentukan nilai yang ingin Anda

perbarui, bersama dengan nama sumber daya dan jenis sinkronisasi. Misalnya, perintah berikut memperbarui nama cabang yang terkait dengan konfigurasi sinkronisasi dengan `--branch` parameter.

```
aws codeconnections update-sync-configuration --sync-type CFN_STACK_SYNC --
resource-name mystack --branch feature-branch
```

2. Perintah ini mengembalikan output berikut.

```
{
  "SyncConfiguration": {
    "Branch": "feature-branch",
    "ConfigFile": "filename.yaml",
    "OwnerId": "owner_id",
    "ProviderType": "GitHub",
    "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
    "RepositoryName": "MyRepo",
    "ResourceName": "mystack",
    "RoleArn": "arn:aws:iam::account_id:role/myrole",
    "SyncType": "CFN_STACK_SYNC"
  }
}
```

Konfigurasi sinkronisasi daftar

Anda dapat menggunakan `list-sync-configurations` perintah di AWS Command Line Interface (AWS CLI) untuk membuat daftar tautan repositori untuk akun Anda.

Untuk membuat daftar tautan repositori

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `list-sync-configurations` perintah, menentukan jenis sinkronisasi dan ID tautan repositori.

```
aws codeconnections list-sync-configurations --repository-link-id
6053346f-8a33-4edb-9397-10394b695173 --sync-type CFN_STACK_SYNC
```

2. Perintah ini mengembalikan output berikut.

```
{
  "SyncConfigurations": [
    {
```

```
    "Branch": "main",
    "ConfigFile": "filename.yaml",
    "OwnerId": "owner_id",
    "ProviderType": "GitHub",
    "RepositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
    "RepositoryName": "MyRepo",
    "ResourceName": "mystack",
    "RoleArn": "arn:aws:iam::account_id:role/myrole",
    "SyncType": "CFN_STACK_SYNC"
  }
]
}
```

Hapus konfigurasi sinkronisasi

Anda dapat menggunakan `delete-sync-configuration` perintah di AWS Command Line Interface (AWS CLI) untuk menghapus konfigurasi sinkronisasi.

Important

Setelah Anda menjalankan perintah, konfigurasi sinkronisasi dihapus. Tidak ada kotak dialog konfirmasi yang ditampilkan. Anda dapat membuat konfigurasi sinkronisasi baru, tetapi Amazon Resource Name (ARN) tidak digunakan kembali.

Untuk menghapus konfigurasi sinkronisasi

- Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `delete-sync-configuration` perintah, menentukan jenis sinkronisasi dan nama sumber daya untuk konfigurasi sinkronisasi yang ingin Anda hapus.

```
aws codeconnections delete-sync-configuration --sync-type CFN_STACK_SYNC --
resource-name mystack
```

Perintah ini tidak mengembalikan apa pun.

Lihat detail konfigurasi sinkronisasi

Anda dapat menggunakan `get-sync-configuration` perintah di AWS Command Line Interface (AWS CLI) untuk melihat detail untuk konfigurasi sinkronisasi.

Untuk melihat detail untuk konfigurasi sinkronisasi

1. Buka terminal (Linux, macOS, atau Unix) atau command prompt (Windows). Gunakan AWS CLI untuk menjalankan `get-sync-configuration` perintah, menentukan ID tautan repositori.

```
aws codeconnections get-sync-configuration --sync-type CFN_STACK_SYNC --resource-name mystack
```

2. Perintah ini mengembalikan output berikut.

```
{
  "SyncConfiguration": {
    "Branch": "main",
    "ConfigFile": "filename",
    "OwnerId": "owner_id",
    "ProviderType": "GitHub",
    "RepositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
    "RepositoryName": "MyRepo",
    "ResourceName": "mystack",
    "RoleArn": "arn:aws:iam::account_id:role/myrole",
    "SyncType": "CFN_STACK_SYNC"
  }
}
```

Pencatatan panggilan AWS CodeConnections API dengan AWS CloudTrail

AWS CodeConnections terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap semua panggilan API untuk notifikasi sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Alat Pengembang dan panggilan kode ke operasi AWS CodeConnections API.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon Simple Storage Service (Amazon S3), termasuk acara untuk notifikasi. 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 AWS CodeConnections, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail lainnya.

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

AWS CodeConnections informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di AWS CodeConnections, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat [Melihat CloudTrail peristiwa dengan riwayat peristiwa](#) di Panduan AWS CloudTrail Pengguna.

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

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna AWS CloudTrail :

- [Ikhtisar untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari berbagai wilayah](#)
- [Menerima file CloudTrail log dari beberapa akun](#)

Semua AWS CodeConnections tindakan dicatat oleh CloudTrail dan didokumentasikan dalam [referensi AWS CodeConnections API](#). Misalnya, panggilan ke `CreateConnection`, `DeleteConnection` dan `GetConnection` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan dibuat dengan root atau kredensial IAM lainnya.

- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Memahami entri file log

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

Contoh **CreateConnection**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateConnection tindakan.

```
{
  "EventId": "b4374fde-c544-4d43-b511-7d899568e55a",
  "EventName": "CreateConnection",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-09T15:13:46-08:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:user/Mary_Major",
```

```

        "accountId": "123456789012",
        "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
        "creationDate": "2024-01-09T23:03:08Z",
        "mfaAuthenticated": "false"
    }
}
},
"eventTime": "2024-01-09T23:13:46Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "CreateConnection",
"awsRegion": "us-east-1",
"sourceIPAddress": "IP",
"userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.create-connection",
"requestParameters": {
    "providerType": "GitHub",
    "connectionName": "my-connection"
},
"responseElements": {
    "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
},
"requestID": "57640a88-97b7-481d-9665-cfd79a681379",
"eventID": "b4374fde-c544-4d43-b511-7d899568e55a",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
    "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
}
}
}

```

Contoh CreateHost

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateHost tindakan.

```
{
```

```
"EventId": "af4ce349-9f21-43fb-8003-267fbf9b1a93",
"EventName": "CreateHost",
"ReadOnly": "false",
"AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
"EventTime": "2024-01-11T12:43:06-08:00",
"EventSource": "codeconnections.amazonaws.com",
"Username": "Mary_Major",
"Resources": [],
"CloudTrailEvent": {
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-01-11T20:09:35Z",
        "mfaAuthenticated": "false"
      }
    }
  }
},
"eventTime": "2024-01-11T20:43:06Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "CreateHost",
"awsRegion": "us-east-1",
"sourceIPAddress": "52.94.133.137",
"userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.create-host",
"requestParameters": {
  "name": "Demo1",
  "providerType": "GitHubEnterpriseServer",
  "providerEndpoint": "IP"
},
"responseElements": {
```

```

    "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
  },
  "requestID": "974459b3-8a04-4cff-9c8f-0c88647831cc",
  "eventID": "af4ce349-9f21-43fb-8003-267fbf9b1a93",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
  }
}
}

```

Contoh **CreateSyncConfiguration**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan **CreateSyncConfiguration** tindakan.

```

{
  "EventId": "be1397e1-eefb-49f0-b4ee-2708c45e94e7",
  "EventName": "CreateSyncConfiguration",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-24T17:38:30+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",

```

```
        "accountId": "123456789012",
        "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
        "creationDate": "2024-01-24T17:34:55Z",
        "mfaAuthenticated": "false"
    }
}
},
"eventTime": "2024-01-24T17:38:30Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "CreateSyncConfiguration",
"awsRegion": "us-east-1",
"sourceIPAddress": "IP",
"userAgent": "aws-cli/2.15.11 Python/3.11.6
Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/offcommand/
codeconnections.create-sync-configuration",
"requestParameters": {
    "branch": "master",
    "configFile": "filename",
    "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
    "resourceName": "mystack",
    "roleArn": "arn:aws:iam::123456789012:role/my-role",
    "syncType": "CFN_STACK_SYNC"
},
"responseElements": {
    "syncConfiguration": {
        "branch": "main",
        "configFile": "filename",
        "ownerId": "owner_ID",
        "providerType": "GitHub",
        "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "repositoryName": "MyGitHubRepo",
        "resourceName": "mystack",
        "roleArn": "arn:aws:iam::123456789012:role/my-role",
        "syncType": "CFN_STACK_SYNC"
    }
},
"requestID": "bad2f662-3f2a-42c0-b638-6115384896f6",
"eventID": "be1397e1-eefb-49f0-b4ee-2708c45e94e7",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
```

```
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}
```

Contoh DeleteConnection

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan DeleteConnection tindakan.

```
{
  "EventId": "672837cd-f977-4fe2-95c7-14280b2af76c",
  "EventName": "DeleteConnection",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-10T13:00:50-08:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::001919387613:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-10T20:41:16Z",
          "mfaAuthenticated": "false"
        }
      }
    }
  }
}
```

```

    },
    "eventTime": "2024-01-10T21:00:50Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "DeleteConnection",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "IP",
    "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.delete-connection",
    "requestParameters": {
      "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
    },
    "responseElements": null,
    "requestID": "4f26ceab-d665-41df-9e15-5ed0fbb4eca6",
    "eventID": "672837cd-f977-4fe2-95c7-14280b2af76c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}

```

Contoh DeleteHost

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan DeleteHost tindakan.

```

{
  "EventId": "6018ba5c-6f24-4a30-b201-16ec19a1687a",
  "EventName": "DeleteHost",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-11T12:56:47-08:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",

```

```

    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-01-11T20:09:35Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-01-11T20:56:47Z",
  "eventSource": "codeconnections.amazonaws.com",
  "eventName": "DeleteHost",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "IP",
  "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.delete-host",
  "requestParameters": {
    "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
  },
  "responseElements": null,
  "requestID": "1b244528-143a-4028-b9a4-9479e342bce5",
  "eventID": "6018ba5c-6f24-4a30-b201-16ec19a1687a",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
  }
}
}

```

Contoh DeleteSyncConfiguration

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan DeleteSyncConfiguration tindakan.

```
{
  "EventId": "588660c7-3202-4998-a906-7bb72bcf4438",
  "EventName": "DeleteSyncConfiguration",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-24T17:41:59+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-24T17:34:55Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "eventTime": "2024-01-24T17:41:59Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "DeleteSyncConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "52.94.133.142",
```

```

    "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.delete-sync-configuration",
    "requestParameters": {
      "syncType": "CFN_STACK_SYNC",
      "resourceName": "mystack"
    },
    "responseElements": null,
    "requestID": "221e0b1c-a50e-4cf0-ab7d-780154e29c94",
    "eventID": "588660c7-3202-4998-a906-7bb72bcf4438",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}

```

Contoh **GetConnection**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan GetConnection tindakan.

```

{
  "EventId": "672837cd-f977-4fe2-95c7-14280b2af76c",
  "EventName": "DeleteConnection",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-10T13:00:50-08:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {

```

```

        "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2024-01-10T20:41:16Z",
            "mfaAuthenticated": "false"
        }
    }
},
"eventTime": "2024-01-10T21:00:50Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "DeleteConnection",
"awsRegion": "us-east-1",
"sourceIPAddress": "IP",
"userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.delete-connection",
"requestParameters": {
    "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/df03df74-8e05-45cf-b420-b39e389dd264"
},
"responseElements": null,
"requestID": "4f26ceab-d665-41df-9e15-5ed0fbb4eca6",
"eventID": "672837cd-f977-4fe2-95c7-14280b2af76c",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "001919387613",
"eventCategory": "Management",
"tlsDetails": {
    "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
}
}
}

```

Contoh **GetHost**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan GetHost tindakan.

```

{
  "EventId": "faa147e7-fe7c-4ab9-a11b-2568a2883c01",
  "EventName": "GetHost",
  "ReadOnly": "true",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-11T12:44:34-08:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-11T20:09:35Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2024-01-11T20:09:35Z",
      "mfaAuthenticated": "false"
    }
  },
  "eventTime": "2024-01-11T20:44:34Z",
  "eventSource": "codeconnections.amazonaws.com",
  "eventName": "GetHost",
  "awsRegion": "us-east-1",
  "sourceIpAddress": "52.94.133.137",
  "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.get-host",
  "requestParameters": {
    "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/Demo1-
EXAMPLE"
  },

```

```

    "responseElements": null,
    "requestID": "0ad61bb6-f88f-4f96-92fe-997f017ec2bb",
    "eventID": "faa147e7-fe7c-4ab9-a11b-2568a2883c01",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}

```

Contoh **GetRepositoryLink**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan GetRepositoryLink tindakan.

```

{
  "EventId": "b46acb67-3612-41c7-8987-adb6c9ed4ad4",
  "EventName": "GetRepositoryLink",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-24T02:59:28+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        }
      }
    }
  },
}

```

```

        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2024-01-24T02:58:52Z",
            "mfaAuthenticated": "false"
        }
    },
    "eventTime": "2024-01-24T02:59:28Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "GetRepositoryLink",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "IP",
    "userAgent": "aws-cli/2.15.11
Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off
command/codeconnections.get-repository-link",
    "requestParameters": {
        "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173"
    },
    "responseElements": {
        "repositoryLinkInfo": {
            "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adeb-4ceaefcb2167",
            "ownerId": "123456789012",
            "providerType": "GitHub",
            "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
            "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
            "repositoryName": "MyGitHubRepo"
        }
    },
    "requestID": "d46704dd-dbe9-462f-96a6-022a8d319fd1",
    "eventID": "b46acb67-3612-41c7-8987-adb6c9ed4ad4",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "api.us-ea-1.codeconnections.aws.dev"
    }
}
}
}

```

Contoh `GetRepositorySyncStatus`

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [GetRepositorySyncStatus](#) tindakan.

```
{
  "EventId": "3e183b74-d8c4-4ad3-9de3-6b5721c522e9",
  "EventName": "GetRepositorySyncStatus",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-25T03:41:44+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-25T02:56:55Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2024-01-25T02:56:55Z",
      "mfaAuthenticated": "false"
    }
  },
  "eventTime": "2024-01-25T03:41:44Z",
  "eventSource": "codeconnections.amazonaws.com",
  "eventName": "GetRepositorySyncStatus",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "52.94.133.138",
```

```

    "userAgent": "aws-cli/2.15.11 Python/3.11.6
Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-repository-sync-status",
    "errorCode": "ResourceNotFoundException",
    "errorMessage": "Could not find a sync status for repository
link:6053346f-8a33-4edb-9397-10394b695173",
    "requestParameters": {
        "branch": "feature-branch",
        "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "syncType": "CFN_STACK_SYNC"
    },
    "responseElements": null,
    "requestID": "e0cee3ee-31e8-4ef5-b749-96cdcabbe36f",
    "eventID": "3e183b74-d8c4-4ad3-9de3-6b5721c522e9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
}
}
}

```

Contoh **GetResourceSyncStatus**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [GetResourceSyncStatus](#) tindakan.

```

{
  "EventId": "9c47054e-f6f6-4345-96d0-9a5af3954a8d",
  "EventName": "GetResourceSyncStatus",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-25T03:44:11+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",

```

```
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-01-25T02:56:55Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-01-25T03:44:11Z",
  "eventSource": "codeconnections.amazonaws.com",
  "eventName": "GetResourceSyncStatus",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "IP",
  "userAgent": "aws-cli/2.15.11 Python/3.11.6
Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-resource-sync-status",
  "requestParameters": {
    "resourceName": "mystack",
    "syncType": "CFN_STACK_SYNC"
  },
  "responseElements": null,
  "requestID": "e74b5503-d651-4920-9fd2-0f40fb5681e0",
  "eventID": "9c47054e-f6f6-4345-96d0-9a5af3954a8d",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
  }
}
```

```
}
```

Contoh **GetSyncBlockerSummary**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [GetSyncBlockerSummary](#) tindakan.

```
{
  "EventId": "c16699ba-a788-476d-8c6c-47511d76309e",
  "EventName": "GetSyncBlockerSummary",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-25T03:03:02+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-25T02:56:55Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "eventTime": "2024-01-25T03:03:02Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "GetSyncBlockerSummary",
    "awsRegion": "us-east-1",
```

```

    "sourceIPAddress": "IP",
    "userAgent": "aws-cli/2.15.11 Python/3.11.6
Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.get-sync-blocker-summary",
    "requestParameters": {
        "syncType": "CFN_STACK_SYNC",
        "resourceName": "mystack"
    },
    "responseElements": {
        "syncBlockerSummary": {
            "resourceName": "mystack",
            "latestBlockers": []
        }
    },
    "requestID": "04240091-eb25-4138-840d-776f8e5375b4",
    "eventID": "c16699ba-a788-476d-8c6c-47511d76309e",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
}
}
}

```

Contoh **GetSyncConfiguration**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [GetSyncConfiguration](#) tindakan.

```

{
    "EventId": "bab9aa16-4553-4206-a1ea-88219233dd25",
    "EventName": "GetSyncConfiguration",
    "ReadOnly": "false",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-24T17:40:40+00:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",
    "Resources": [],
    "CloudTrailEvent": {
        "eventVersion": "1.08",
        "userIdentity": {

```

```

    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-01-24T17:34:55Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-01-24T17:40:40Z",
  "eventSource": "codeconnections.amazonaws.com",
  "eventName": "GetSyncConfiguration",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "52.94.133.142",
  "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.get-sync-configuration",
  "requestParameters": {
    "syncType": "CFN_STACK_SYNC",
    "resourceName": "mystack"
  },
  "responseElements": {
    "syncConfiguration": {
      "branch": "main",
      "configFile": "filename",
      "ownerId": "123456789012",
      "providerType": "GitHub",
      "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
      "repositoryName": "MyGitHubRepo",
      "resourceName": "mystack",
      "roleArn": "arn:aws:iam::123456789012:role/my-role",
      "syncType": "CFN_STACK_SYNC"
    }
  }
}

```

```

    },
    "requestID": "0aa8e43a-6e34-4d8f-89fb-5c2d01964b35",
    "eventID": "bab9aa16-4553-4206-a1ea-88219233dd25",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}

```

Contoh **ListConnections**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [ListConnections](#) tindakan.

```

{
  "EventId": "3f8d80fe-fbe1-4755-903c-4f58fc8262fa",
  "EventName": "ListConnections",
  "ReadOnly": "true",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-08T14:11:23-08:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        }
      }
    }
  },

```

```

        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2024-01-08T22:11:02Z",
            "mfaAuthenticated": "false"
        }
    },
    "eventTime": "2024-01-08T22:11:23Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "ListConnections",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "IP",
    "userAgent": "aws-cli/1.18.147 Python/2.7.18
Linux/5.10.201-168.748.amzn2int.x86_64 boto-core/1.18.6",
    "requestParameters": {
        "maxResults": 50
    },
    "responseElements": null,
    "requestID": "5d456d59-3e92-44be-b941-a429df59e90b",
    "eventID": "3f8d80fe-fbe1-4755-903c-4f58fc8262fa",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
}
}

```

Contoh **ListHosts**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [ListHosts](#) tindakan.

```

{
    "EventId": "f6e9e831-feaf-4ad1-ac47-51681109c401",
    "EventName": "ListHosts",
    "ReadOnly": "true",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "EventTime": "2024-01-11T13:00:55-08:00",
    "EventSource": "codeconnections.amazonaws.com",
    "Username": "Mary_Major",

```

```
"Resources": [],
"CloudTrailEvent": {
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-01-11T20:09:35Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-01-11T21:00:55Z",
  "eventSource": "codeconnections.amazonaws.com",
  "eventName": "ListHosts",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "IP",
  "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.list-hosts",
  "requestParameters": {
    "maxResults": 50
  },
  "responseElements": null,
  "requestID": "ea87e2cf-6bf1-4cc7-9666-f3fad85d6d83",
  "eventID": "f6e9e831-feaf-4ad1-ac47-51681109c401",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
```

```

    }
  }
}

```

Contoh `ListRepositoryLinks`

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [ListRepositoryLinks](#) tindakan.

```

{
  "EventId": "4f714bbb-0716-4f6e-9868-9b379b30757f",
  "EventName": "ListRepositoryLinks",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-24T01:57:29+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-24T01:43:49Z",
          "mfaAuthenticated": "false"
        }
      }
    }
  },
  "eventTime": "2024-01-24T01:57:29Z",
  "eventSource": "codeconnections.amazonaws.com",
  "eventName": "ListRepositoryLinks",

```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "IP",
    "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.list-repository-links",
    "requestParameters": {
      "maxResults": 50
    },
    "responseElements": {
      "repositoryLinks": [
        {
          "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/001f5be2-a661-46a4-b96b-4d277cac8b6e",
          "ownerId": "123456789012",
          "providerType": "GitHub",
          "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/be8f2017-b016-4a77-87b4-608054f70e77",
          "repositoryLinkId": "be8f2017-b016-4a77-87b4-608054f70e77",
          "repositoryName": "MyGitHubRepo"
        },
        {
          "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adeb-4ceaefcb2167",
          "ownerId": "owner",
          "providerType": "GitHub",
          "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
          "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
          "repositoryName": "MyGitHubRepo"
        }
      ]
    },
    "requestID": "7c8967a9-ec15-42e9-876b-0ef58681ec55",
    "eventID": "4f714bbb-0716-4f6e-9868-9b379b30757f",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}
```

```
}
```

Contoh `ListRepositorySyncDefinitions`

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [ListRepositorySyncDefinitions](#) tindakan.

```
{
  "EventId": "12e52dbb-b00d-49ad-875a-3efec36e5aa1",
  "EventName": "ListRepositorySyncDefinitions",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-25T16:56:19+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-25T16:43:03Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "eventTime": "2024-01-25T16:56:19Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "ListRepositorySyncDefinitions",
    "awsRegion": "us-east-1",
```

```

    "sourceIPAddress": "IP",
    "userAgent": "aws-cli/2.15.11 Python/3.11.6
Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.list-repository-sync-definitions",
    "requestParameters": {
        "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "syncType": "CFN_STACK_SYNC",
        "maxResults": 50
    },
    "responseElements": {
        "repositorySyncDefinitions": []
    },
    "requestID": "df31d11d-5dc7-459b-9a8f-396b4769cdd9",
    "eventID": "12e52dbb-b00d-49ad-875a-3efec36e5aa1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
}

```

Contoh **ListSyncConfigurations**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [ListSyncConfiguration](#) tindakan.

```

{
  "EventId": "aa4ae557-ec31-4151-8d21-9e74dd01344c",
  "EventName": "ListSyncConfigurations",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-24T17:42:06+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",

```

```
"arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "creationDate": "2024-01-24T17:34:55Z",
    "mfaAuthenticated": "false"
  }
},
"eventTime": "2024-01-24T17:42:06Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "ListSyncConfigurations",
"awsRegion": "us-east-1",
"sourceIPAddress": "IP",
"userAgent": "aws-cli/2.15.11 Python/3.11.6
Linux/5.10.205-172.804.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/offcommand/
codeconnections.list-sync-configurations",
"requestParameters": {
  "maxResults": 50,
  "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
  "syncType": "CFN_STACK_SYNC"
},
"responseElements": {
  "syncConfigurations": [
    {
      "branch": "feature-branch",
      "configFile": "filename.yaml",
      "ownerId": "owner",
      "providerType": "GitHub",
      "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
      "repositoryName": "MyGitHubRepo",
      "resourceName": "dkstacksync",
      "roleArn": "arn:aws:iam::123456789012:role/my-role",
      "syncType": "CFN_STACK_SYNC"
    }
  ]
}
```

```

    ]
  },
  "requestID": "7dd220b5-fc0f-4023-aaa0-9555cfe759df",
  "eventID": "aa4ae557-ec31-4151-8d21-9e74dd01344c",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
  }
}
}

```

Contoh `ListTagsForResource`

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [ListTagsForResource](#) tindakan.

```

{
  "EventId": "fc501054-d68a-4325-824c-0e34062ef040",
  "EventName": "ListTagsForResource",
  "ReadOnly": "true",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-25T17:16:56+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "dMary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        }
      }
    }
  }
}

```

```

    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2024-01-25T16:43:03Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2024-01-25T17:16:56Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "ListTagsForResource",
"awsRegion": "us-east-1",
"sourceIPAddress": "IP",
"userAgent": "aws-cli/2.15.11 Python/3.11.6
Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.list-tags-for-resource",
"requestParameters": {
  "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/9703702f-bebe-41b7-8fc4-8e6d2430a330"
},
"responseElements": null,
"requestID": "994584a3-4807-47f2-bb1b-a64f0af6c250",
"eventID": "fc501054-d68a-4325-824c-0e34062ef040",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
}
}
}

```

Contoh TagResource

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [TagResource](#) tindakan.

```

{
  "EventId": "b7fbc943-2dd1-4c5b-a5ad-fc6d60a011f1",
  "EventName": "TagResource",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",

```

```
"EventTime": "2024-01-11T12:22:11-08:00",
"EventSource": "codeconnections.amazonaws.com",
"Username": "Mary_Major",
"Resources": [],
"CloudTrailEvent": {
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-01-11T20:09:35Z",
        "mfaAuthenticated": "false"
      }
    }
  },
},
"eventTime": "2024-01-11T20:22:11Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "TagResource",
"awsRegion": "us-east-1",
"sourceIPAddress": "IP",
"userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.tag-resource",
"requestParameters": {
  "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/8dcf69d1-3316-4392-ae09-71e038adb6ed",
  "tags": [
    {
      "key": "Demo1",
      "value": "hhvh1"
    }
  ]
},
},
```

```

    "responseElements": null,
    "requestID": "ba382c33-7124-48c8-a23a-25816ce27604",
    "eventID": "b7fbc943-2dd1-4c5b-a5ad-fc6d60a011f1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}

```

Contoh **UntagResource**

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [UntagResource](#) tindakan.

```

{
  "EventId": "8a85cdee-2586-4679-be18-eec34204bc7e",
  "EventName": "UntagResource",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-11T12:31:14-08:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        }
      }
    },
  },
}

```

```

        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2024-01-11T20:09:35Z",
            "mfaAuthenticated": "false"
        }
    },
    "eventTime": "2024-01-11T20:31:14Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "IP",
    "userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.untag-resource",
    "requestParameters": {
        "resourceArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/8dcf69d1-3316-4392-ae09-71e038adb6ed",
        "tagKeys": [
            "Project",
            "ReadOnly"
        ]
    },
    "responseElements": null,
    "requestID": "05ef26a4-8c39-4f72-89bf-0c056c51b8d7",
    "eventID": "8a85cdee-2586-4679-be18-eec34204bc7e",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
}
}

```

Contoh UpdateHost

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [UpdateHost](#) tindakan.

```

"Events": [{
    "EventId": "4307cf7d-6d1c-40d9-a659-1bb41b31a2b6",
    "EventName": "UpdateHost",

```

```

"readOnly": "false",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"eventTime": "2024-01-11T12:54:32-08:00",
"eventSource": "codeconnections.amazonaws.com",
"username": "Mary_Major",
"resources": [],
"cloudTrailEvent": "eventVersion": "1.08",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AIDACKCEVSQ6C2EXAMPLE",
  "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
  "accountId": "123456789012",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:role/Admin",
      "accountId": "123456789012",
      "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2024-01-11T20:09:35Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2024-01-11T20:54:32Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "UpdateHost",
"awsRegion": "us-east-1",
"sourceIpAddress": "IP",
"userAgent": "aws-cli/2.13.30 Python/3.11.6 Darwin/23.2.0 exe/x86_64 prompt/off
command/codeconnections.update-host",
"requestParameters": {
  "hostArn": "arn:aws:codeconnections:us-east-1:123456789012:host/
Demo1-34e70ecb",
  "providerEndpoint": "https://54.218.245.167"
},
"responseElements": null,
"requestID": "b17f46ac-1acb-44ab-a9f5-c35c20233441",
"eventID": "4307cf7d-6d1c-40d9-a659-1bb41b31a2b6",
"readOnly": false,

```

```
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
}
```

Contoh UpdateRepositoryLink

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [UpdateRepositoryLink](#) tindakan.

```
{
  "EventId": "be358c9a-5a8f-467e-8585-2860070be4fe",
  "EventName": "UpdateRepositoryLink",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-24T02:03:24+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-24T01:43:49Z",
          "mfaAuthenticated": "false"
        }
      }
    }
  }
}
```

```
    },
    "eventTime": "2024-01-24T02:03:24Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "UpdateRepositoryLink",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "IP",
    "userAgent": "aws-
cli/2.15.11Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/
offcommand/codeconnections.update-repository-link",
    "requestParameters": {
      "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adeb-4ceaefcb2167",
      "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173"
    },
    "responseElements": {
      "repositoryLinkInfo": {
        "connectionArn": "arn:aws:codeconnections:us-
east-1:123456789012:connection/7df263cc-f055-4843-adeb-4ceaefcb2167",
        "ownerId": "owner",
        "providerType": "GitHub",
        "repositoryLinkArn": "arn:aws:codeconnections:us-
east-1:123456789012:repository-link/6053346f-8a33-4edb-9397-10394b695173",
        "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
        "repositoryName": "MyGitHubRepo"
      }
    },
    "additionalEventData": {
      "providerAction": "UpdateRepositoryLink"
    },
    "requestID": "e01eee49-9393-4983-89e4-d1b3353a70d9",
    "eventID": "be358c9a-5a8f-467e-8585-2860070be4fe",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}
```

Contoh UpdateSyncBlocker

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [UpdateSyncBlocker](#) tindakan.

```
{
  "EventId": "211d19db-9f71-4d93-bf90-10f9ddefed88",
  "EventName": "UpdateSyncBlocker",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-25T03:01:05+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::123456789012:role/Admin",
          "accountId": "123456789012",
          "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
          "creationDate": "2024-01-25T02:56:55Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "eventTime": "2024-01-25T03:01:05Z",
    "eventSource": "codeconnections.amazonaws.com",
    "eventName": "UpdateSyncBlocker",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "IP",
    "userAgent": "aws-cli/2.15.11 Python/3.11.6
Linux/5.10.205-172.807.amzn2int.x86_64 exe/x86_64.amzn.2 prompt/off command/
codeconnections.update-sync-blocker",
```

```

    "requestParameters": {
      "id": "ID",
      "syncType": "CFN_STACK_SYNC",
      "resourceName": "mystack",
      "resolvedReason": "Reason"
    },
    "responseElements": null,
    "requestID": "eea03b39-b299-4099-ba55-608480f8d96d",
    "eventID": "211d19db-9f71-4d93-bf90-10f9ddefed88",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"
    }
  }
}

```

Contoh UpdateSyncConfiguration

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [UpdateSyncConfiguration](#) tindakan.

```

{
  "EventId": "d961c94f-1881-4fe8-83bf-d04cb9f22577",
  "EventName": "UpdateSyncConfiguration",
  "ReadOnly": "false",
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "EventTime": "2024-01-24T17:40:55+00:00",
  "EventSource": "codeconnections.amazonaws.com",
  "Username": "Mary_Major",
  "Resources": [],
  "CloudTrailEvent": {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/Mary_Major",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {

```

```

    "sessionIssuer": {
      "type": "Role",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:role/Admin",
      "accountId": "123456789012",
      "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2024-01-24T17:34:55Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2024-01-24T17:40:55Z",
"eventSource": "codeconnections.amazonaws.com",
"eventName": "UpdateSyncConfiguration",
"awsRegion": "us-east-1",
"sourceIPAddress": "IP",
"userAgent": "aws-cli/2.15.11
Python/3.11.6Linux/5.10.205-172.804.amzn2int.x86_64exe/x86_64.amzn.2prompt/offcommand/
codeconnections.update-sync-configuration",
"requestParameters": {
  "branch": "feature-branch",
  "resourceName": "mystack",
  "syncType": "CFN_STACK_SYNC"
},
"responseElements": {
  "syncConfiguration": {
    "branch": "feature-branch",
    "configFile": "filename",
    "ownerId": "owner",
    "providerType": "GitHub",
    "repositoryLinkId": "6053346f-8a33-4edb-9397-10394b695173",
    "repositoryName": "MyGitHubRepo",
    "resourceName": "mystack",
    "roleArn": "arn:aws:iam::123456789012:role/my-role",
    "syncType": "CFN_STACK_SYNC"
  }
},
"requestID": "2ca545ef-4395-4e1f-b14a-2750481161d6",
"eventID": "d961c94f-1881-4fe8-83bf-d04cb9f22577",
"readOnly": false,
"eventType": "AwsApiCall",

```

```
    "managementEvent": true,  
    "recipientAccountId": "123456789012",  
    "eventCategory": "Management",  
    "tlsDetails": {  
      "clientProvidedHostHeader": "api.us-east-1.codeconnections.aws.dev"  
    }  
  }  
}
```

AWS CodeConnections dan antarmuka titik akhir VPC (AWS PrivateLink)

Anda dapat membuat koneksi pribadi antara VPC Anda dan AWS CodeConnections dengan membuat antarmuka VPC endpoint. Endpoint antarmuka didukung oleh [AWS PrivateLink](#), teknologi yang memungkinkan Anda mengakses secara pribadi AWS CodeConnections APIs tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi Direct AWS Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk AWS CodeConnections APIs berkomunikasi, karena lalu lintas antara VPC Anda AWS CodeConnections dan tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa [Antarmuka Jaringan Elastis](#) di subnet Anda.

Untuk informasi selengkapnya, lihat [Antarmuka VPC endpoint \(AWS PrivateLink\)](#) dalam Panduan Pengguna Amazon VPC.

Pertimbangan untuk titik akhir AWS CodeConnections VPC

Sebelum menyiapkan titik akhir VPC antarmuka AWS CodeConnections, pastikan Anda meninjau titik [akhir Antarmuka di](#) Panduan Pengguna Amazon VPC.

AWS CodeConnections mendukung panggilan ke semua tindakan API-nya dari VPC Anda.

Titik akhir VPC didukung di semua Wilayah. AWS CodeConnections

Konsep VPC endpoint

Berikut ini adalah konsep utama untuk VPC endpoint:

Titik akhir VPC

Titik masuk di VPC Anda yang memungkinkan Anda untuk terhubung secara pribadi ke layanan. Berikut ini adalah berbagai jenis VPC endpoint. Anda membuat jenis VPC endpoint yang diperlukan oleh layanan yang didukung.

- [Titik akhir VPC untuk tindakan AWS CodeConnections](#)
- [Titik akhir VPC untuk webhook AWS CodeConnections](#)

AWS PrivateLink

Sebuah teknologi yang menyediakan konektivitas pribadi antara VPCs dan layanan.

Titik akhir VPC untuk tindakan AWS CodeConnections

Anda dapat mengelola titik akhir VPC untuk layanan ini. AWS CodeConnections

Membuat titik akhir VPC antarmuka untuk tindakan AWS CodeConnections

Anda dapat membuat titik akhir VPC untuk AWS CodeConnections layanan menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat [Membuat titik akhir antarmuka](#) dalam Panduan Pengguna Amazon VPC.

Untuk mulai menggunakan koneksi dengan VPC Anda, buat antarmuka VPC endpoint untuk. AWS CodeConnections Saat Anda membuat titik akhir VPC untuk AWS CodeConnections, pilih AWS Layanan, dan di Nama Layanan, pilih:

- `com.amazonaws. region.codestar-connections.api`: Opsi ini membuat titik akhir VPC untuk operasi API. AWS CodeConnections Misalnya, pilih opsi ini jika pengguna Anda menggunakan AWS CLI, AWS CodeConnections API, atau AWS SDKs untuk berinteraksi dengan AWS CodeConnections untuk operasi seperti `CreateConnection`, `ListConnections`, dan `CreateHost`

Untuk opsi Aktifkan nama DNS, jika Anda memilih DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API untuk AWS CodeConnections menggunakan nama DNS default untuk Wilayah, misalnya, `.codestar-connections.us-east-1.amazonaws.com`

Important

DNS pribadi diaktifkan secara default untuk endpoint yang dibuat untuk AWS layanan dan layanan AWS Marketplace Partner.

Untuk informasi selengkapnya, lihat [Mengakses layanan melalui titik akhir antarmuka](#) dalam Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk tindakan AWS CodeConnections

Anda dapat melampirkan kebijakan titik akhir ke VPC endpoint yang mengendalikan akses ke AWS CodeConnections. Kebijakan menentukan informasi berikut ini:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat [Mengontrol Akses ke Layanan dengan titik akhir VPC](#) dalam Panduan Pengguna Amazon VPC.

Note

Com.amazonaws.*region*.codestar-connections.webhooks endpoint tidak mendukung kebijakan.

Contoh: Kebijakan titik akhir VPC untuk tindakan AWS CodeConnections

Berikut ini adalah contoh kebijakan endpoint untuk AWS CodeConnections. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke AWS CodeConnections tindakan yang tercantum untuk semua prinsipal di semua sumber daya.

```
{
  "Statement": [
    {
      "Sid": "GetConnectionOnly",
      "Principal": "*",
      "Action": [
        "codestar-connections:GetConnection"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Titik akhir VPC untuk webhook AWS CodeConnections

AWS CodeConnections membuat titik akhir webhook untuk Anda saat Anda membuat atau menghapus host dengan konfigurasi VPC. Nama endpoint adalah `com.amazonaws.region.codestar-connections.webhooks`.

Dengan titik akhir VPC untuk GitHub webhook, host dapat mengirim data peristiwa melalui webhook ke layanan terintegrasi Anda melalui jaringan Amazon. AWS

Important

Saat menyiapkan host untuk GitHub Enterprise Server, AWS CodeConnections buat titik akhir VPC untuk data peristiwa webhooks untuk Anda. Jika Anda membuat host sebelum 24 November 2020, dan Anda ingin menggunakan titik akhir PrivateLink webhook VPC, Anda harus terlebih dahulu [menghapus](#) host Anda dan kemudian [membuat](#) host baru.

AWS CodeConnections mengelola siklus hidup titik akhir ini. Untuk menghapus titik akhir, Anda harus menghapus sumber daya host yang sesuai.

Bagaimana titik akhir webhook untuk AWS CodeConnections host digunakan

Titik akhir webhook adalah tempat webhook dari repositori pihak ketiga dikirim untuk diproses. AWS CodeConnections Sebuah webhook menggambarkan tindakan pelanggan. Ketika Anda melakukan `git push`, titik akhir webhook menerima webhook dari penyedia yang merinci push. Misalnya, AWS CodeConnections dapat memberi tahu CodePipeline untuk memulai pipeline Anda.

Untuk penyedia cloud, seperti Bitbucket, atau host Server GitHub Enterprise yang tidak menggunakan VPC, titik akhir VPC webhook tidak berlaku karena penyedia mengirim webhook ke AWS CodeConnections tempat jaringan Amazon tidak digunakan.

Pemecahan masalah koneksi

Informasi berikut dapat membantu Anda memecahkan masalah umum dengan koneksi ke sumber daya di AWS CodeBuild, AWS CodeDeploy, dan. AWS CodePipeline

Topik

- [Saya tidak dapat membuat koneksi](#)

- [Saya mendapatkan kesalahan izin saat mencoba membuat atau menyelesaikan koneksi](#)
- [Saya mendapatkan kesalahan izin saat mencoba menggunakan koneksi](#)
- [Koneksi tidak dalam status tersedia atau tidak lagi tertunda](#)
- [Tambahkan GitClone izin untuk koneksi](#)
- [Host tidak dalam status tersedia](#)
- [Memecahkan masalah host dengan kesalahan koneksi](#)
- [Saya tidak dapat membuat koneksi untuk host saya](#)
- [Pemecahan masalah konfigurasi VPC untuk host Anda](#)
- [Pemecahan masalah titik akhir PrivateLink VPC webhook \(\) untuk koneksi Server Perusahaan GitHub](#)
- [Pemecahan masalah untuk host yang dibuat sebelum 24 November 2020](#)
- [Tidak dapat membuat koneksi untuk GitHub repositori](#)
- [Edit izin aplikasi koneksi GitHub Enterprise Server Anda](#)
- [Kesalahan koneksi saat menghubungkan ke GitHub: “Masalah terjadi, pastikan cookie diaktifkan di browser Anda” atau “Pemilik organisasi harus menginstal GitHub aplikasi”](#)
- [Awalan layanan koneksi di sumber daya mungkin perlu diperbarui untuk kebijakan IAM](#)
- [Kesalahan izin karena awalan layanan di sumber daya yang dibuat menggunakan konsol](#)
- [Koneksi dan penyiapan host untuk penyedia terinstal yang mendukung organisasi](#)
- [Saya ingin meningkatkan batas saya untuk koneksi](#)

Saya tidak dapat membuat koneksi

Anda mungkin tidak memiliki izin untuk membuat koneksi. Untuk informasi lebih lanjut, lihat [Izin dan contoh untuk AWS CodeConnections](#).

Saya mendapatkan kesalahan izin saat mencoba membuat atau menyelesaikan koneksi

Pesan galat berikut mungkin akan ditampilkan saat Anda mencoba membuat atau melihat sambungan di CodePipeline konsol.

Pengguna: *username* tidak berwenang untuk melakukan: *permission* pada sumber daya: *connection-ARN*

Jika pesan ini muncul, pastikan bahwa Anda memiliki izin yang memadai.

Izin untuk membuat dan melihat koneksi di AWS Command Line Interface (AWS CLI) atau hanya bagian dari izin yang Anda perlukan untuk membuat dan menyelesaikan koneksi di konsol. Konsol Manajemen AWS Izin yang diperlukan untuk hanya melihat, mengedit, atau membuat koneksi dan kemudian menyelesaikan koneksi yang tertunda harus dicakupkan ke bawah untuk pengguna yang hanya perlu melakukan tugas-tugas tertentu. Untuk informasi lebih lanjut, lihat [Izin dan contoh untuk AWS CodeConnections](#).

Saya mendapatkan kesalahan izin saat mencoba menggunakan koneksi

Salah satu atau kedua pesan kesalahan berikut mungkin dikembalikan jika Anda mencoba menggunakan koneksi di CodePipeline konsol, meskipun Anda memiliki izin untuk membuat daftar, mendapatkan, dan membuat izin.

Anda gagal mengautentikasi akun Anda.

Pengguna: *username* tidak berwenang untuk melakukan: codestar-connections: on resource: UseConnection *connection-ARN*

Jika hal ini terjadi, pastikan bahwa Anda memiliki izin yang memadai.

Pastikan Anda memiliki izin untuk menggunakan koneksi, termasuk mencantumkan repositori yang tersedia di lokasi penyedia. Untuk informasi lebih lanjut, lihat [Izin dan contoh untuk AWS CodeConnections](#).

Koneksi tidak dalam status tersedia atau tidak lagi tertunda

Jika konsol menampilkan pesan bahwa koneksi tidak dalam status tersedia, pilih Selesaikan koneksi.

Jika Anda memilih untuk menyelesaikan koneksi dan muncul pesan bahwa koneksi tidak dalam status tertunda, Anda dapat membatalkan permintaan karena koneksi sudah dalam status tersedia.

Tambahkan GitClone izin untuk koneksi

Saat Anda menggunakan AWS CodeStar koneksi dalam aksi sumber dan CodeBuild tindakan, ada dua cara artefak input dapat diteruskan ke build:

- Default: Tindakan sumber menghasilkan file zip yang berisi kode yang CodeBuild diunduh.
- Klon Git: Kode sumber dapat langsung diunduh ke lingkungan pembangunan.

Mode klon Git memungkinkan Anda untuk berinteraksi dengan kode sumber sebagai repositori Git yang berfungsi. Untuk menggunakan mode ini, Anda harus memberikan izin CodeBuild lingkungan Anda untuk menggunakan koneksi.

Untuk menambahkan izin ke kebijakan peran CodeBuild layanan, Anda membuat kebijakan terkelola pelanggan yang dilampirkan ke peran CodeBuild layanan. Langkah-langkah berikut membuat kebijakan di mana izin `UseConnection` ditentukan di bidang `action`, dan koneksi Amazon Resource Name (ARN) ditentukan di bidang `Resource`.

Untuk menggunakan konsol untuk menambahkan `UseConnection` izin

1. Untuk menemukan ARN koneksi untuk alur Anda, buka alur Anda dan pilih ikon (i) pada tindakan sumber Anda. Panel Konfigurasi terbuka, dan koneksi ARN muncul di sebelah. `ConnectionArn` Anda menambahkan ARN koneksi ke kebijakan peran CodeBuild layanan Anda.
2. Untuk menemukan peran CodeBuild layanan Anda, buka proyek build yang digunakan dalam pipeline Anda dan navigasikan ke tab Detail build.
3. Di bagian Lingkungan, pilih tautan Peran layanan. Ini membuka konsol AWS Identity and Access Management (IAM), tempat Anda dapat menambahkan kebijakan baru yang memberikan akses ke koneksi Anda.
4. Pada konsol IAM, pilih Lampirkan kebijakan, lalu pilih Buat kebijakan.

Gunakan templat kebijakan sampel berikut. Tambahkan ARN koneksi Anda di bidang `Resource`, seperti yang ditunjukkan dalam contoh ini.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "codestar-connections:UseConnection",
      "Resource": "arn:aws:iam::*:role/Service*"
    }
  ]
}
```

Pada tab JSON, tempel kebijakan Anda.

5. Pilih Tinjau kebijakan. Masukkan nama untuk kebijakan (misalnya, **connection-permissions**), lalu pilih Buat kebijakan.
6. Kembali ke halaman Lampirkan Izin peran layanan, segarkan daftar kebijakan, dan pilih kebijakan yang baru saja Anda buat. Pilih Lampirkan kebijakan.

Host tidak dalam status tersedia

Jika konsol menampilkan pesan bahwa host tidak dalam status `Available`, pilih Menyiapkan host.

Langkah pertama untuk pembuatan host menghasilkan host yang dibuat sekarang dalam status `Pending`. Untuk memindahkan host ke status `Available`, Anda harus memilih untuk menyiapkan host di konsol. Untuk informasi selengkapnya, lihat [Menyiapkan host yang tertunda](#).

Note

Anda tidak dapat menggunakan AWS CLI untuk mengatur host. `Pending`

Memecahkan masalah host dengan kesalahan koneksi

Koneksi dan host dapat beralih ke status kesalahan jika GitHub aplikasi yang mendasarinya dihapus atau dimodifikasi. Host dan koneksi dalam status kesalahan tidak dapat dipulihkan dan host harus dibuat ulang.

- Tindakan seperti mengubah kunci pem aplikasi, mengubah nama aplikasi (setelah pembuatan awal) akan menyebabkan host dan semua koneksi terkait masuk ke status kesalahan.

Jika konsol atau CLI mengembalikan host atau koneksi yang terkait dengan host dengan status `Error`, Anda mungkin perlu melakukan langkah berikut:

- Hapus dan buat ulang sumber daya host dan kemudian instal ulang aplikasi pendaftaran host. Untuk informasi lebih lanjut, lihat [Membuat host](#).

Saya tidak dapat membuat koneksi untuk host saya

Untuk membuat koneksi atau host, syarat-syarat berikut diperlukan.

- Host Anda harus dalam status TERSEDIA. Untuk informasi selengkapnya, lihat
- Koneksi harus dibuat di Wilayah yang sama dengan host.

Pemecahan masalah konfigurasi VPC untuk host Anda

Saat membuat sumber daya host, Anda harus menyediakan koneksi jaringan atau informasi VPC untuk infrastruktur tempat instans Server GitHub Perusahaan Anda diinstal. Untuk memecahkan masalah konfigurasi VPC atau subnet untuk host Anda, gunakan contoh informasi VPC yang ditampilkan di sini sebagai referensi.

Note

Gunakan bagian ini untuk pemecahan masalah yang terkait dengan konfigurasi host Server GitHub Perusahaan Anda dalam VPC Amazon. Untuk pemecahan masalah yang terkait dengan koneksi Anda yang dikonfigurasi untuk menggunakan titik akhir webhook untuk PrivateLink VPC (), lihat. [Pemecahan masalah titik akhir PrivateLink VPC webhook \(\) untuk koneksi Server Perusahaan GitHub](#)

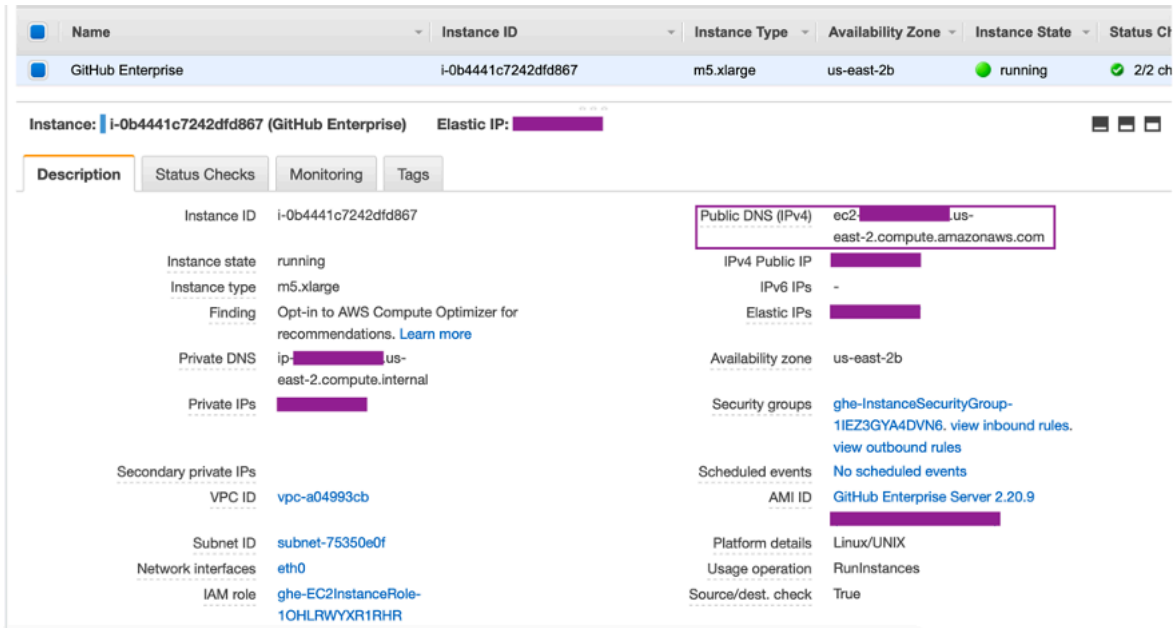
Untuk contoh ini, Anda akan menggunakan proses berikut untuk mengkonfigurasi VPC dan server tempat instance GitHub Enterprise Server Anda akan diinstal:

1. Membuat VPC. Untuk informasi lebih lanjut, lihat <https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#Create-VPC>.
2. Membuat subnet di VPC Anda. Untuk informasi lebih lanjut, lihat <https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#AddSubnet>.
3. Meluncurkan instans ke VPC Anda. Untuk informasi selengkapnya, lihat https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#VPC_Launch_Instance.

Note

Setiap VPC hanya dapat dikaitkan dengan satu host (contoh Server GitHub Perusahaan) pada satu waktu.

Gambar berikut menunjukkan instans EC2 yang diluncurkan menggunakan AMI GitHub Perusahaan.



Saat Anda menggunakan VPC untuk koneksi GitHub Enterprise Server, Anda harus memberikan yang berikut untuk infrastruktur saat menyiapkan host:

- ID VPC: VPC untuk server tempat instans Server GitHub Perusahaan Anda diinstal atau VPC yang memiliki akses ke instance Server GitHub Perusahaan yang diinstal melalui VPN atau Direct Connect.
- Subnet ID atau IDs: Subnet untuk server tempat instans Server GitHub Enterprise Anda diinstal atau subnet dengan akses ke instance GitHub Enterprise Server yang diinstal melalui VPN atau Direct Connect.
- Grup atau grup keamanan: Grup keamanan untuk server tempat instans Server GitHub Perusahaan Anda diinstal atau grup keamanan dengan akses ke instans Server GitHub Perusahaan yang diinstal melalui VPN atau Direct Connect.
- Titik akhir: Siapkan titik akhir server Anda dan lanjutkan ke langkah berikutnya.

Untuk informasi selengkapnya tentang bekerja dengan VPCs dan subnet, lihat Ukuran [VPC dan Subnet untuk IPv4 di Panduan Pengguna Amazon VPC](#).

Topik

- [Saya tidak bisa mendapatkan host dalam status tertunda](#)
- [Saya tidak bisa mendapatkan host dalam status tersedia](#)

- [Saya connection/host sedang bekerja dan telah berhenti bekerja sekarang](#)
- [Saya tidak dapat menghapus antarmuka jaringan saya](#)

Saya tidak bisa mendapatkan host dalam status tertunda

Jika host Anda memasuki status `VPC_CONFIG_FAILED_INITIALIZATION`, hal ini mungkin karena masalah dengan VPC, subnet, atau grup keamanan yang telah Anda pilih untuk host Anda.

- VPC, subnet, dan grup keamanan semuanya harus dimiliki oleh akun yang membuat host.
- Subnet dan grup keamanan harus milik VPC yang dipilih.
- Setiap subnet yang disediakan harus berada di Availability Zone yang berbeda.
- Pengguna yang membuat host harus memiliki izin IAM berikut:

```
ec2:CreateNetworkInterface
ec2:CreateTags
ec2:DescribeDhcpOptionsec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2>DeleteNetworkInterface
ec2:DescribeVpcs
ec2:CreateVpcEndpoint
ec2>DeleteVpcEndpoints
ec2:DescribeVpcEndpoints
```

Saya tidak bisa mendapatkan host dalam status tersedia

Jika Anda tidak dapat menyelesaikan penyiapan CodeConnections aplikasi untuk host Anda, itu mungkin karena masalah dengan konfigurasi VPC atau instance Server GitHub Perusahaan Anda.

- Jika Anda tidak menggunakan otoritas sertifikat publik, Anda harus memberikan sertifikat TLS kepada host Anda yang digunakan oleh Instans GitHub Perusahaan Anda. Nilai Sertifikat TLS harus menjadi kunci publik sertifikat.
- Anda harus menjadi administrator instance GitHub Enterprise Server untuk membuat GitHub aplikasi.

Saya connection/host sedang bekerja dan telah berhenti bekerja sekarang

Jika a berfungsi connection/host sebelumnya dan tidak berfungsi sekarang, itu mungkin karena perubahan konfigurasi di VPC Anda atau GitHub aplikasi telah dimodifikasi. Periksa hal-hal berikut:

- Grup keamanan yang dilampirkan ke sumber daya host yang Anda buat untuk koneksi Anda kini telah berubah atau tidak lagi memiliki akses ke Server GitHub Perusahaan. CodeConnections memerlukan grup keamanan yang memiliki konektivitas ke instance GitHub Enterprise Server.
- IP Server DNS baru-baru ini berubah. Anda dapat memverifikasi ini dengan memeriksa opsi DHCP yang dilampirkan ke VPC yang ditentukan dalam sumber daya host yang Anda buat untuk koneksi Anda. Perhatikan bahwa jika Anda baru saja pindah dari AmazonProvided DNS ke Server DNS khusus atau mulai menggunakan Server DNS kustom baru, itu host/connection akan berhenti berfungsi. Untuk memperbaikinya, hapus host Anda yang ada dan buat ulang, yang akan menyimpan pengaturan DNS terbaru di basis data kami.
- ACLs Pengaturan jaringan telah berubah dan tidak lagi mengizinkan koneksi HTTP ke subnet tempat infrastruktur Server GitHub Perusahaan Anda berada.
- Konfigurasi CodeConnections aplikasi apa pun di Server GitHub Perusahaan Anda telah berubah. Modifikasi pada konfigurasi apa pun, seperti URLs atau rahasia aplikasi, dapat memutus konektivitas antara instans Server GitHub Perusahaan yang diinstal dan CodeConnections.

Saya tidak dapat menghapus antarmuka jaringan saya

Jika Anda tidak dapat mendeteksi antarmuka jaringan Anda, periksa hal berikut:

- Antarmuka Jaringan yang dibuat oleh hanya CodeConnections dapat dihapus dengan menghapus host. Mereka tidak dapat dihapus secara manual oleh pengguna.
- Anda harus memiliki izin berikut:

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Pemecahan masalah titik akhir PrivateLink VPC webhook () untuk koneksi Server Perusahaan GitHub

Saat Anda membuat host dengan konfigurasi VPC, VPC endpoint webhook dibuat untuk Anda.

Note

Gunakan bagian ini untuk pemecahan masalah yang terkait dengan koneksi Anda yang dikonfigurasi untuk menggunakan titik akhir webhook untuk VPC (). PrivateLink Untuk

pemecahan masalah yang terkait dengan konfigurasi host Server GitHub Perusahaan Anda dalam VPC Amazon, lihat. [Pemecahan masalah konfigurasi VPC untuk host Anda](#)

Ketika Anda membuat koneksi ke jenis penyedia yang diinstal, dan Anda telah menentukan bahwa server Anda dikonfigurasi dalam VPC, kemudian AWS CodeConnections membuat host Anda, dan titik akhir VPC (PrivateLink) untuk webhook dibuat untuk Anda. Ini memungkinkan host untuk mengirim data peristiwa melalui webhook ke AWS layanan terintegrasi Anda melalui jaringan Amazon. Untuk informasi selengkapnya, lihat [AWS CodeConnections dan antarmuka titik akhir VPC \(\)AWS PrivateLink](#).

Topik

- [Saya tidak dapat menghapus VPC endpoint webhook saya](#)

Saya tidak dapat menghapus VPC endpoint webhook saya

AWS CodeConnections mengelola siklus hidup titik akhir VPC webhook untuk host Anda. Jika Anda ingin menghapus titik akhir, Anda harus melakukan ini dengan menghapus sumber daya host yang sesuai.

- [Titik akhir VPC webhook PrivateLink \(\) yang dibuat CodeConnections oleh hanya dapat dihapus dengan menghapus host](#). Mereka tidak dapat dihapus secara manual.
- Anda harus memiliki izin berikut:

```
ec2:DescribeNetworkInterfaces
ec2:DeleteNetworkInterface
```

Pemecahan masalah untuk host yang dibuat sebelum 24 November 2020

Mulai 24 November 2020, saat AWS CodeConnections menyiapkan host Anda, dukungan titik akhir (PrivateLink) VPC tambahan disiapkan untuk Anda. Untuk host yang dibuat sebelum pembaruan ini, gunakan bagian pemecahan masalah ini.

Untuk informasi lebih lanjut, lihat [AWS CodeConnections dan antarmuka titik akhir VPC \(\)AWS PrivateLink](#).

Topik

- [Saya memiliki host yang dibuat sebelum 24 November 2020 dan saya ingin menggunakan titik akhir VPC \(\) PrivateLink untuk webhook](#)
- [Saya tidak bisa mendapatkan host dalam status tersedia \(kesalahan VPC\)](#)

Saya memiliki host yang dibuat sebelum 24 November 2020 dan saya ingin menggunakan titik akhir VPC () PrivateLink untuk webhook

Ketika Anda mengatur host Anda untuk GitHub Enterprise Server, titik akhir webhook dibuat untuk Anda. Koneksi sekarang menggunakan titik akhir PrivateLink webhook VPC. Jika Anda membuat host sebelum 24 November 2020, dan Anda ingin menggunakan titik akhir PrivateLink webhook VPC, Anda harus terlebih dahulu [menghapus](#) host Anda dan kemudian [membuat](#) host baru.

Saya tidak bisa mendapatkan host dalam status tersedia (kesalahan VPC)

Jika host Anda dibuat sebelum 24 November 2020, dan Anda tidak dapat menyelesaikan penyiapan CodeConnections aplikasi untuk host Anda, itu mungkin karena masalah dengan konfigurasi VPC atau instance Server GitHub Perusahaan Anda.

VPC Anda akan memerlukan NAT Gateway (atau akses internet keluar) sehingga instance Server GitHub Perusahaan Anda dapat mengirim lalu lintas jaringan keluar untuk webhook. GitHub

Tidak dapat membuat koneksi untuk GitHub repositori

Masalah:

Karena koneksi ke GitHub repositori menggunakan AWS Connector for GitHub, Anda memerlukan izin pemilik organisasi atau izin admin ke repositori untuk membuat koneksi.

Kemungkinan perbaikan: [Untuk informasi tentang tingkat izin untuk GitHub repositori, lihat https://docs.github.com/en/free-pro-team@latest/github/setting-up-and-managing-organizations-and-teams/permission-levels-for-an-organization](https://docs.github.com/en/free-pro-team@latest/github/setting-up-and-managing-organizations-and-teams/permission-levels-for-an-organization)

Edit izin aplikasi koneksi GitHub Enterprise Server Anda

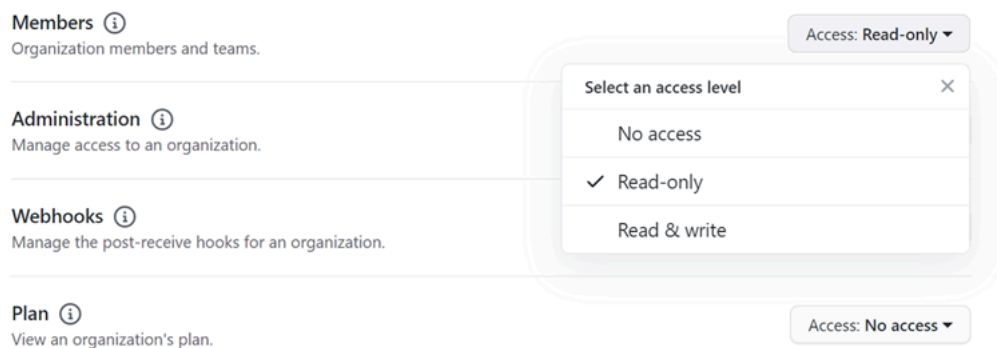
Jika Anda menginstal aplikasi untuk Server GitHub Perusahaan pada atau sebelum 23 Desember 2020, Anda mungkin perlu memberikan akses hanya-baca aplikasi ke anggota organisasi. Jika Anda adalah pemilik GitHub aplikasi, ikuti langkah-langkah berikut untuk mengedit izin untuk aplikasi yang diinstal saat host Anda dibuat.

Note

Anda harus menyelesaikan langkah-langkah ini pada instance GitHub Enterprise Server Anda, dan Anda harus menjadi pemilik GitHub aplikasi.

1. Di Server GitHub Perusahaan, dari opsi drop-down pada foto profil Anda, pilih Pengaturan.
2. Pilih Pengaturan pengembang, lalu pilih GitHubAplikasi.
3. Dalam daftar aplikasi, pilih nama aplikasi untuk koneksi Anda, lalu pilih Izin dan peristiwa di tampilan pengaturan.
4. Pada Izin organisasi, untuk Anggota, pilih Hanya-baca dari tarik-bawah Akses.

Organization permissions



5. Di Menambahkan catatan ke pengguna, tambahkan deskripsi alasan pembaruan. Pilih Simpan perubahan.

Kesalahan koneksi saat menghubungkan ke GitHub: “Masalah terjadi, pastikan cookie diaktifkan di browser Anda” atau “Pemilik organisasi harus menginstal GitHub aplikasi”

Masalah:

Untuk membuat koneksi untuk GitHub repositori, Anda harus menjadi pemilik GitHub organisasi. Untuk repositori yang tidak berada di bawah organisasi, Anda harus menjadi pemilik repositori. Ketika koneksi dibuat oleh orang lain selain pemilik organisasi, permintaan dibuat untuk pemilik organisasi, dan salah satu kesalahan berikut akan ditampilkan:

Masalah terjadi, pastikan cookie diaktifkan di browser Anda

ATAU

Pemilik organisasi harus menginstal GitHub aplikasi

Kemungkinan perbaikan: Untuk repositori dalam GitHub organisasi, pemilik organisasi harus membuat koneksi ke repositori. GitHub Untuk repositori yang tidak berada di bawah organisasi, Anda harus menjadi pemilik repositori.

Awalan layanan koneksi di sumber daya mungkin perlu diperbarui untuk kebijakan IAM

Pada 29 Maret 2024, layanan ini diubah namanya dari AWS CodeStar Connections menjadi. AWS CodeConnections Mulai 1 Juli 2024, konsol membuat koneksi dengan `codeconnections` ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol. Awalan layanan untuk sumber daya yang dibuat menggunakan konsol adalah `codeconnections`. SDK/CLI Sumber daya baru dibuat dengan `codeconnections` ARN sumber daya. Sumber daya yang dibuat akan secara otomatis memiliki awalan layanan baru.

Berikut ini adalah sumber daya yang dibuat di AWS CodeConnections:

- Koneksi
- Host

Masalah:

Sumber daya yang telah dibuat dengan `codestar-connections` di ARN tidak akan secara otomatis diganti namanya menjadi awalan layanan baru di sumber daya ARN. Membuat sumber daya baru akan membuat sumber daya yang memiliki awalan layanan koneksi. Namun, kebijakan IAM dengan awalan `codestar-connections` layanan tidak akan berfungsi untuk sumber daya dengan awalan layanan baru.

Kemungkinan perbaikan: Untuk menghindari masalah akses atau izin untuk sumber daya, selesaikan tindakan berikut:

- Perbarui kebijakan IAM untuk awalan layanan baru. Jika tidak, sumber daya yang diganti namanya atau dibuat tidak akan dapat menggunakan kebijakan IAM.
- Perbarui sumber daya untuk awalan layanan baru dengan membuatnya menggunakan konsol atau CLI/CDK/CFN.

Perbarui tindakan, sumber daya, dan ketentuan dalam kebijakan yang sesuai. Dalam contoh berikut, Resource bidang telah diperbarui untuk kedua awalan layanan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "codeconnections:UseConnection"
    ],
    "Resource": [
      "arn:aws:codestar-connections:*:*:connection/*",
      "arn:aws:codeconnections:*:*:connection/*"
    ]
  }
}
```

Kesalahan izin karena awalan layanan di sumber daya yang dibuat menggunakan konsol

Saat ini, sumber daya koneksi yang dibuat menggunakan konsol hanya akan memiliki awalan `codestar-connections` layanan. Untuk sumber daya yang dibuat menggunakan konsol, tindakan pernyataan kebijakan harus disertakan `codestar-connections` sebagai awalan layanan.

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan `codeconnections` ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Masalah:

Saat membuat sumber daya koneksi menggunakan konsol, awalan `codestar-connections` layanan harus digunakan dalam kebijakan. Saat menggunakan kebijakan dengan awalan `codeconnections` layanan dalam kebijakan, sumber daya koneksi yang dibuat menggunakan konsol menerima pesan galat berikut:

```
User: user_ARN is not authorized to perform: codestar-connections:action on
resource: resource_ARN because no identity-based policy allows the codestar-
connections:action action
```

Kemungkinan perbaikan: Untuk sumber daya yang dibuat menggunakan konsol, tindakan pernyataan kebijakan harus disertakan `codestar-connections` sebagai awalan layanan, seperti yang ditunjukkan dalam contoh kebijakan di [Contoh: Kebijakan untuk membuat AWS CodeConnections dengan konsol](#)

Koneksi dan penyiapan host untuk penyedia terinstal yang mendukung organisasi

Untuk penyedia terinstal yang mendukung organisasi, seperti GitHub Organizations, Anda tidak melewati host yang tersedia. Anda membuat host baru untuk setiap koneksi di organisasi Anda dan pastikan untuk memasukkan informasi yang sama di bidang jaringan berikut:

- ID VPC
- ID Subnet
- Grup keamanan IDs

Lihat langkah-langkah terkait untuk membuat koneksi [GHES atau koneksi](#) yang [GitLab dikelola sendiri](#).

Saya ingin meningkatkan batas saya untuk koneksi

Anda dapat meminta kenaikan batas untuk batas tertentu di CodeConnections. Lihat informasi yang lebih lengkap di [Kuota untuk koneksi](#).

Kuota untuk koneksi

Tabel berikut mencantumkan kuota (juga disebut sebagai batas) untuk koneksi dalam konsol Alat Developer.

Kuota dalam tabel ini berlaku per Wilayah AWS dan dapat ditingkatkan. Untuk Wilayah AWS informasi dan kuota yang dapat diubah, lihat [kuota AWS layanan](#).

Note

Anda harus mengaktifkan Eropa (Milan) Wilayah AWS sebelum Anda dapat menggunakannya. Untuk informasi selengkapnya, lihat [Mengaktifkan Wilayah](#).

Sumber Daya	Batas default
Jumlah maksimum koneksi per Akun AWS	250

Kuota dalam tabel ini tetap dan tidak dapat diubah.

Sumber Daya	Batas default
Karakter maksimum dalam nama koneksi	32 karakter
Jumlah maksimum host per Akun AWS	50
Jumlah maksimum tautan repositori	100
Jumlah maksimum konfigurasi sinkronisasi CloudFormation tumpukan	100
Jumlah maksimum konfigurasi sinkronisasi per tautan repositori	100
Jumlah maksimum konfigurasi sinkronisasi per cabang	50

Alamat IP untuk ditambahkan ke daftar izin Anda

Jika Anda menerapkan pemfilteran IP, atau mengizinkan alamat IP tertentu di EC2 instans Amazon, tambahkan alamat IP berikut ke daftar izin Anda. Melakukan hal itu memungkinkan koneksi ke penyedia, seperti GitHub dan Bitbucket.

Tabel berikut mencantumkan alamat IP untuk koneksi di konsol Alat Pengembang oleh Wilayah AWS.

Note

Untuk Wilayah Eropa (Milan), Anda harus mengaktifkan Wilayah ini sebelum Anda dapat menggunakannya. Untuk informasi selengkapnya, lihat [Mengaktifkan Wilayah](#).

Wilayah	Alamat IP
AS Barat (Oregon) (us-west-2)	35.160.210.199, 54.71.206.108, 54.71.36.205
AS Timur (Virginia Utara) (us-east-1)	3.216.216.90, 3.216.243.220, 3.217.241.85
Eropa (Irlandia) (eu-west-1)	34.242.64.82, 52.18.37.201, 54.77.75.62
AS Timur (Ohio) (us-east-2)	18.217.188.190, 18.218.158.91, 18.220.4.80
Asia Pasifik (Singapura) (ap-southeast-1)	18.138.171.151, 18.139.22.70, 3.1.157.176
Asia Pasifik (Sydney) (ap-southeast-2)	13.236.59.253, 52.64.166.86, 54.206.1.112
Asia Pasifik (Tokyo) (ap-northeast-1)	52.196.132.231, 54.95.133.227, 18.181.13.91
Eropa (Frankfurt) (eu-central-1)	18.196.145.164, 3.121.252.59, 52.59.104.195
Asia Pasifik (Seoul) (ap-northeast-2)	13.125.8.239, 13.209.223.177, 3.37.200.23
Asia Pasifik (Mumbai) (ap-south-1)	13.234.199.152, 13.235.29.220, 35.154.23 0.124
Amerika Selatan (Sao Paulo) (sa-east-1)	18.229.77.26, 54.233.226.52, 54.233.207.69
Kanada (Pusat) (ca-central-1)	15.222.219.210, 35.182.166.138, 99.79.111 .198
Eropa (London) (eu-west-2)	3.9.97.205, 35.177.150.185, 35.177.200.225
AS Barat (California Utara) (us-west-1)	52.52.16.175, 52.8.63.87
Eropa (Paris) (eu-west-3)	35.181.127.138, 35.181.145.22, 35.181.20.200
Eropa (Stockholm) (eu-north-1)	13.48.66.148, 13.48.8.79, 13.53.78.182
Europe (Milan) (eu-south-1)	18.102.28.105, 18.102.35.130, 18.102.8.116
AWS GovCloud (AS-Timur)	18.252.168.157, 18.252.207.77, 18.253.18 5.119

Keamanan untuk fitur konsol Alat Developer

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](#) menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di 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 berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS CodeStar Pemberitahuan dan AWS CodeConnections, lihat [AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan](#).
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS CodeStar Notifikasi dan AWS CodeConnections. Topik berikut menunjukkan kepada Anda cara mengonfigurasi AWS CodeStar Pemberitahuan dan AWS CodeConnections untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan AWS CodeStar Pemberitahuan dan AWS CodeConnections sumber daya Anda.

Untuk informasi selengkapnya tentang keamanan untuk layanan di konsol Alat Developer, lihat berikut ini:

- [CodeBuild Keamanan](#)
- [CodeCommit Keamanan](#)
- [CodeDeploy Keamanan](#)
- [CodePipeline Keamanan](#)

Memahami konten dan keamanan notifikasi

Notifikasi memberikan informasi tentang sumber daya kepada pengguna yang berlangganan target aturan notifikasi yang Anda konfigurasi. Informasi ini dapat mencakup detail tentang sumber daya alat developer Anda, termasuk isi repositori, membangun status, status deployment, dan eksekusi alur.

Misalnya, Anda dapat mengonfigurasi aturan notifikasi untuk repositori CodeCommit untuk menyertakan komentar pada commit atau pull request. Jika demikian, notifikasi yang dikirim dalam menanggapi aturan tersebut mungkin berisi baris atau baris kode yang direferensikan dalam komentar tersebut. Demikian pula, Anda dapat mengonfigurasi aturan notifikasi untuk proyek build CodeBuild agar menyertakan keberhasilan atau kegagalan untuk status dan fase build. Notifikasi yang dikirim dalam menanggapi aturan tersebut akan berisi informasi tersebut.

Anda dapat mengonfigurasi aturan notifikasi untuk pipeline CodePipeline untuk menyertakan informasi tentang persetujuan manual, dan notifikasi yang dikirim sebagai tanggapan terhadap aturan tersebut mungkin berisi nama orang yang memberikan persetujuan tersebut. Anda dapat mengonfigurasi aturan notifikasi untuk aplikasi CodeDeploy untuk menunjukkan keberhasilan penerapan, dan notifikasi yang dikirim sebagai respons terhadap aturan tersebut mungkin berisi informasi tentang target penerapan.

Notifikasi dapat mencakup informasi spesifik proyek seperti status build, baris kode yang memiliki komentar, status deployment, dan persetujuan alur. Jadi untuk membantu memastikan keamanan proyek Anda, pastikan bahwa Anda secara teratur meninjau kedua target aturan notifikasi dan daftar pelanggan dari topik Amazon SNS yang ditetapkan sebagai target. Selain itu, konten notifikasi yang dikirim sebagai respons terhadap peristiwa dapat berubah karena fitur tambahan ditambahkan ke layanan dasar. Perubahan ini dapat terjadi tanpa pemberitahuan untuk aturan notifikasi yang sudah ada. Pertimbangkan untuk meninjau isi pesan notifikasi secara berkala untuk membantu memastikan bahwa Anda memahami apa yang sedang dikirim, serta kepada siapa pesan tersebut dikirim.

Untuk informasi selengkapnya tentang tipe peristiwa yang tersedia untuk aturan notifikasi, lihat [Konsep notifikasi](#).

Anda dapat memilih untuk membatasi detail yang disertakan dalam notifikasi hanya pada apa yang disertakan dalam suatu peristiwa. Ini disebut sebagai tipe detail Basic. Peristiwa ini berisi informasi yang persis sama seperti yang dikirim ke Amazon EventBridge dan Amazon CloudWatch Events.

Layanan konsol Alat Pengembang, seperti CodeCommit, dapat memilih untuk menambahkan informasi tentang beberapa atau semua jenis acara mereka dalam pesan notifikasi di luar apa

yang tersedia dalam suatu acara. Informasi tambahan ini dapat ditambahkan kapan saja untuk meningkatkan jenis peristiwa saat ini atau melengkapi jenis peristiwa di masa mendatang. Anda dapat memilih untuk menyertakan informasi tambahan tentang peristiwa tersebut, jika tersedia, dalam notifikasi dengan memilih tipe detail Penuh. Untuk informasi selengkapnya, lihat [Jenis detail](#).

Perlindungan data di AWS CodeStar Pemberitahuan dan AWS CodeConnections

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di AWS CodeStar Pemberitahuan dan AWS CodeConnections. 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. Untuk informasi selengkapnya tentang privasi data, lihat [FAQ Privasi Data AWS](#). Untuk informasi tentang perlindungan data di Eropa, lihat [Pusat Peraturan Umum Perlindungan Data \(GDPR\)](#).

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

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

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS CodeStar Notifikasi dan AWS CodeConnections 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.

Manajemen identitas dan akses untuk AWS CodeStar Pemberitahuan dan AWS CodeConnections

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

Note

Tindakan untuk sumber daya yang dibuat di bawah awalan layanan baru codeconnections tersedia. Membuat sumber daya di bawah awalan layanan baru akan digunakan codeconnections di sumber daya ARN. Tindakan dan sumber daya untuk awalan codestar-connections layanan tetap tersedia. Saat menentukan sumber daya dalam kebijakan IAM, awalan layanan harus sesuai dengan sumber daya.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana fitur di konsol alat developer bekerja dengan IAM](#)
- [AWS CodeConnections referensi izin](#)
- [Contoh kebijakan berbasis identitas](#)
- [Menggunakan tag untuk mengontrol akses ke AWS CodeConnections sumber daya](#)

- [Menggunakan notifikasi dan koneksi di konsol](#)
- [Izinkan para pengguna untuk melihat izin mereka sendiri](#)
- [Pemecahan Masalah AWS CodeStar Pemberitahuan dan AWS CodeConnections identitas dan akses](#)
- [Menggunakan peran terkait layanan untuk Pemberitahuan AWS CodeStar](#)
- [Menggunakan peran terkait layanan untuk AWS CodeConnections](#)
- [AWS kebijakan terkelola untuk AWS CodeConnections](#)

Audiens

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

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Pemecahan Masalah AWS CodeStar Pemberitahuan dan AWS CodeConnections identitas dan akses](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana fitur di konsol alat developer bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Contoh kebijakan berbasis identitas](#))

Mengautentikasi dengan identitas

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

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

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

Pengguna root akun AWS

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

Pengguna dan grup IAM

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

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

Peran IAM

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

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

Mengelola akses menggunakan kebijakan

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

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

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

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Bagaimana fitur di konsol alat developer bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke fitur di konsol Alat Developer, Anda harus memahami fitur IAM mana yang tersedia untuk digunakan dengannya. Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja notifikasi dan AWS layanan lain dengan IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Topik

- [Kebijakan berbasis identitas di konsol alat developer](#)
- [AWS CodeStar Pemberitahuan dan kebijakan AWS CodeConnections berbasis sumber daya](#)
- [Otorisasi berdasarkan tanda](#)
- [Peran IAM](#)

Kebijakan berbasis identitas di konsol alat developer

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya

tindakan tersebut. AWS CodeStar Pemberitahuan dan AWS CodeConnections mendukung tindakan, sumber daya, dan kunci kondisi tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan IAM JSON](#) dalam Panduan Pengguna IAM.

Tindakan

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

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

Tindakan kebijakan untuk notifikasi di konsol Alat Developer menggunakan prefiks berikut sebelum tindakan: `codestar-notifications` and `codeconnections`. Misalnya, untuk memberikan izin kepada seseorang untuk melihat semua aturan notifikasi di akunnya, Anda menyertakan tindakan `codestar-notifications:ListNotificationRules` dalam kebijakan mereka. Pernyataan kebijakan harus mencakup salah satu `Action` atau `NotAction` elemen. AWS CodeStar Pemberitahuan dan AWS CodeConnections mendefinisikan serangkaian tindakannya sendiri yang menggambarkan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menentukan beberapa tindakan AWS CodeStar Pemberitahuan dalam satu pernyataan, pisahkan dengan koma sebagai berikut.

```
"Action": [  
    "codestar-notifications:action1",  
    "codestar-notifications:action2"
```

Untuk menentukan beberapa AWS CodeConnections tindakan dalam satu pernyataan, pisahkan dengan koma sebagai berikut.

```
"Action": [  
    "codeconnections:action1",  
    "codeconnections:action2"
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata `List`, sertakan tindakan berikut.

```
"Action": "codestar-notifications:List*"
```

AWS CodeStar Tindakan API Pemberitahuan meliputi:

- `CreateNotificationRule`
- `DeleteNotificationRule`
- `DeleteTarget`
- `DescribeNotificationRule`
- `ListEventTypes`
- `ListNotificationRules`
- `ListTagsForResource`
- `ListTargets`
- `Subscribe`
- `TagResource`
- `Unsubscribe`
- `UntagResource`
- `UpdateNotificationRule`

AWS CodeConnections Tindakan API meliputi yang berikut:

- `CreateConnection`
- `DeleteConnection`
- `GetConnection`
- `ListConnections`
- `ListTagsForResource`
- `TagResource`
- `UntagResource`

Tindakan khusus izin berikut diperlukan AWS CodeConnections untuk menyelesaikan jabatan tangan autentikasi:

- `GetIndividualAccessToken`
- `GetInstallationUrl`
- `ListInstallationTargets`

- `StartOAuthHandshake`
- `UpdateConnectionInstallation`

Tindakan khusus izin berikut diperlukan AWS CodeConnections untuk menggunakan koneksi:

- `UseConnection`

Tindakan khusus izin berikut diperlukan AWS CodeConnections untuk meneruskan koneksi ke layanan:

- `PassConnection`

Untuk melihat daftar AWS CodeStar Pemberitahuan dan AWS CodeConnections tindakan, lihat [Tindakan yang Ditentukan oleh AWS CodeStar Pemberitahuan](#) dan [Tindakan yang Ditentukan oleh AWS CodeConnections](#) dalam Panduan Pengguna IAM.

Sumber daya

AWS CodeStar Pemberitahuan dan AWS CodeConnections tidak mendukung menentukan sumber daya ARNs dalam kebijakan.

Kunci syarat

AWS CodeStar Pemberitahuan dan AWS CodeConnections tentukan set kunci kondisi mereka sendiri dan juga mendukung penggunaan beberapa tombol kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Semua tindakan AWS CodeStar Pemberitahuan mendukung tombol `codestar-notifications:NotificationsForResource` kondisi. Untuk informasi selengkapnya, lihat [Contoh kebijakan berbasis identitas](#).

AWS CodeConnections mendefinisikan kunci kondisi berikut yang dapat digunakan dalam `Condition` elemen kebijakan IAM. Anda dapat menggunakan kunci ini untuk menyempurnakan syarat lebih lanjut dimana pernyataan kebijakan berlaku. Untuk informasi lebih lanjut, lihat [AWS CodeConnections referensi izin](#).

Kunci kondisi	Deskripsi
<code>codeconnections:BranchName</code>	Memfilter akses berdasarkan nama cabang repositori pihak ketiga
<code>codeconnections:FullRepositoryId</code>	Memfilter akses berdasarkan repositori yang dilewatkan dalam permintaan. Hanya berlaku untuk permintaan <code>UseConnection</code> untuk akses ke repositori tertentu
<code>codeconnections:InstallationId</code>	Memfilter akses berdasarkan ID pihak ketiga (seperti ID penginstalan aplikasi Bitbucket) yang digunakan untuk memperbarui koneksi. Memungkinkan Anda untuk membatasi instalasi aplikasi pihak ketiga mana yang dapat digunakan untuk membuat koneksi
<code>codeconnections:OwnerId</code>	Memfilter akses berdasarkan pemilik atau ID akun penyedia pihak ketiga
<code>codeconnections:PassedToService</code>	Memfilter akses berdasarkan layanan di mana prinsipal diizinkan untuk melewati koneksi
<code>codeconnections:ProviderAction</code>	Memfilter akses berdasarkan tindakan penyedia di permintaan <code>UseConnection</code> seperti <code>ListRepositories</code> .
<code>codeconnections:ProviderPermissionsRequired</code>	Memfilter akses berdasarkan jenis izin penyedia pihak ketiga
<code>codeconnections:ProviderType</code>	Memfilter akses berdasarkan jenis penyedia pihak ketiga yang dilewatkan dalam permintaan
<code>codeconnections:ProviderTypeFilter</code>	Memfilter akses berdasarkan jenis penyedia pihak ketiga yang dilewatkan dalam hasil filter
<code>codeconnections:RepositoryName</code>	Memfilter akses berdasarkan nama repositori pihak ketiga

Contoh

Untuk melihat contoh AWS CodeStar Pemberitahuan dan kebijakan AWS CodeConnections berbasis identitas, lihat. [Contoh kebijakan berbasis identitas](#)

AWS CodeStar Pemberitahuan dan kebijakan AWS CodeConnections berbasis sumber daya

AWS CodeStar Pemberitahuan dan AWS CodeConnections tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tanda

Anda dapat melampirkan tag ke AWS CodeStar Pemberitahuan dan AWS CodeConnections sumber daya atau meneruskan tag dalam permintaan. Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `codestar-notifications` and `codeconnections:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`. Untuk informasi selengkapnya tentang strategi penandaan, lihat [AWS Menandai](#) sumber daya. Untuk informasi selengkapnya tentang menandai AWS CodeStar Pemberitahuan dan AWS CodeConnections sumber daya, lihat [Menandai sumber daya koneksi](#).

Untuk melihat contoh kebijakan-kebijakan berbasis identitas untuk membatasi akses ke sumber daya berdasarkan tanda pada sumber daya tersebut, lihat [Menggunakan tag untuk mengontrol akses ke AWS CodeConnections sumber daya](#).

Peran IAM

[Peran IAM](#) adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensial sementara

Anda dapat menggunakan kredensial sementara untuk masuk dengan federasi, dan dan mengambil IAM role atau peran lintas-akun. Anda memperoleh kredensi keamanan sementara dengan memanggil operasi AWS STS API seperti [AssumeRole](#) atau. [GetFederationToken](#)

AWS CodeStar Pemberitahuan dan AWS CodeConnections mendukung penggunaan kredensial sementara.

Peran terkait layanan

[Peran terkait AWS layanan](#) memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

AWS CodeStar Pemberitahuan mendukung peran terkait layanan. Untuk detail tentang membuat atau mengelola AWS CodeStar Pemberitahuan dan peran AWS CodeConnections terkait layanan, lihat [Menggunakan peran terkait layanan untuk Pemberitahuan AWS CodeStar](#)

CodeConnections tidak mendukung peran terkait layanan.

AWS CodeConnections referensi izin

Tabel berikut mencantumkan setiap operasi AWS CodeConnections API, tindakan terkait yang dapat Anda berikan izin, dan format ARN sumber daya yang akan digunakan untuk memberikan izin. AWS CodeConnections APIs Dikelompokkan ke dalam tabel berdasarkan cakupan tindakan yang diizinkan oleh API tersebut. Mengacu saat menulis kebijakan izin yang dapat Anda lampirkan ke identitas IAM (kebijakan berbasis identitas).

Ketika Anda membuat kebijakan izin, Anda menentukan tindakan di bidang `Action`. Anda menentukan nilai sumber daya di bidang `Resource` sebagai ARN, dengan atau tanpa karakter wildcard (*).

Untuk mengekspresikan syarat dalam kebijakan koneksi Anda, gunakan kunci syarat yang dijelaskan di sini dan tercantum dalam [Kunci syarat](#). Anda juga dapat menggunakan tombol kondisi AWS-wide. Untuk daftar lengkap tombol AWS-wide, lihat Kunci yang [tersedia](#) di Panduan Pengguna IAM.

Untuk menentukan tindakan, gunakan awalan `codeconnections` yang diikuti dengan nama operasi API (misalnya, `codeconnections:ListConnections` atau `codeconnections:CreateConnection`).

Menggunakan wildcard

Untuk menentukan beberapa tindakan atau sumber daya, gunakan karakter wildcard (*) di ARN Anda. Misalnya, `codeconnections:*` menentukan semua AWS CodeConnections tindakan dan `codeconnections:Get*` menentukan semua AWS CodeConnections tindakan yang dimulai dengan kata. `Get` Contoh berikut memberikan akses ke semua sumber daya dengan nama yang dimulai dengan `MyConnection`.

```
arn:aws:codeconnections:us-west-2:account-ID:connection/*
```

Anda dapat menggunakan wildcard hanya dengan *connection* sumber daya yang tercantum dalam tabel berikut. Anda tidak dapat menggunakan wildcard dengan *region* atau *account-id* sumber daya. Untuk informasi lebih lanjut tentang wildcard, lihat [Pengidentifikasi IAM](#) dalam Panduan Pengguna IAM.

Topik

- [Izin untuk mengelola koneksi](#)
- [Izin untuk mengelola host](#)
- [Izin untuk menyelesaikan koneksi](#)
- [Izin untuk menyiapkan host](#)
- [Melewati koneksi ke layanan](#)
- [Menggunakan koneksi](#)
- [Jenis akses yang didukung untuk ProviderAction](#)
- [Izin yang didukung untuk menandai sumber daya koneksi](#)
- [Melewati koneksi ke tautan repositori](#)
- [Kunci kondisi yang didukung untuk tautan repositori](#)
- [Izin yang didukung untuk berbagi koneksi](#)

Izin untuk mengelola koneksi

Peran atau pengguna yang ditunjuk untuk menggunakan AWS CLI atau SDK untuk melihat, membuat, atau menghapus koneksi harus memiliki izin terbatas pada hal berikut.

Note

Anda tidak dapat menyelesaikan atau menggunakan koneksi di konsol dengan hanya izin berikut. Anda perlu menambahkan izin di [Izin untuk menyelesaikan koneksi](#).

```
codeconnections:CreateConnection  
codeconnections>DeleteConnection  
codeconnections:GetConnection  
codeconnections:ListConnections
```

AWS CodeStar Pemberitahuan dan izin AWS CodeConnections yang diperlukan untuk tindakan untuk mengelola koneksi

CreateConnection

Tindakan: `codeconnections:CreateConnection`

Diperlukan untuk menggunakan CLI atau konsol untuk membuat koneksi.

Resource:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

DeleteConnection

Tindakan: `codeconnections>DeleteConnection`

Diperlukan untuk menggunakan CLI atau konsol untuk menghapus koneksi.

Resource:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

GetConnection

Tindakan: `codeconnections:GetConnection`

Diperlukan untuk menggunakan CLI atau konsol untuk melihat detail tentang koneksi.

Resource:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListConnections

Tindakan: `codeconnections:ListConnections`

Diperlukan untuk menggunakan CLI atau konsol untuk membuat daftar semua koneksi di akun.

Resource:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

Operasi ini mendukung kunci syarat berikut:

Tindakan	Kunci kondisi
<code>codeconnections:CreateConnection</code>	<code>codeconnections:ProviderType</code>

Tindakan	Kunci kondisi
<code>codeconnections:DeleteConnection</code>	N/A
<code>codeconnections:GetConnection</code>	N/A
<code>codeconnections:ListConnections</code>	<code>codeconnections:ProviderTypeFilter</code>

Izin untuk mengelola host

Peran atau pengguna yang ditunjuk untuk menggunakan AWS CLI atau SDK untuk melihat, membuat, atau menghapus host harus memiliki izin terbatas pada hal berikut.

Note

Anda tidak dapat menyelesaikan atau menggunakan koneksi di host dengan hanya izin berikut. Anda perlu menambahkan izin di [Izin untuk menyiapkan host](#).

```
codeconnections:CreateHost
codeconnections>DeleteHost
codeconnections:GetHost
codeconnections:ListHosts
```

AWS CodeStar Pemberitahuan dan izin yang AWS CodeConnections diperlukan untuk tindakan mengelola host

CreateHost

Tindakan: `codeconnections:CreateHost`

Diperlukan untuk menggunakan CLI atau konsol untuk membuat host.

Resource: `arn:aws:codeconnections:region:account-id:host/host-id`

DeleteHost

Tindakan: `codeconnections>DeleteHost`

Diperlukan untuk menggunakan CLI atau konsol untuk menghapus host.

Resource:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

GetHost

Tindakan: codeconnections:GetHost

Diperlukan untuk menggunakan CLI atau konsol untuk melihat detail tentang host.

Resource:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

ListHosts

Tindakan: codeconnections:ListHosts

Diperlukan untuk menggunakan CLI atau konsol untuk membuat daftar semua host di akun.

Resource:arn:aws:codeconnections:*region*:*account-id*:host/*host-id*

Operasi ini mendukung kunci syarat berikut:

Tindakan	Kunci kondisi
codeconnections:CreateHost	codeconnections:ProviderType codeconnections:VpcId
codeconnections>DeleteHost	N/A
codeconnections:GetHost	N/A
codeconnections:ListHosts	codeconnections:ProviderTypeFilter

Untuk contoh kebijakan yang menggunakan kunci VpcIdkondisi, lihat [Contoh: Batasi izin VPC host menggunakan tombol konteks VpcId](#).

Izin untuk menyelesaikan koneksi

Peran atau pengguna yang ditunjuk untuk mengelola koneksi di konsol harus memiliki izin yang diperlukan untuk menyelesaikan koneksi di konsol dan membuat instalasi, yang mencakup otorisasi handshake ke penyedia dan membuat instalasi untuk koneksi untuk digunakan. Gunakan izin berikut selain izin di atas.

Operasi IAM berikut digunakan oleh konsol saat melakukan handshake berbasis browser. `ListInstallationTargets`, `GetInstallationUrl`, `StartOAuthHandshake`, `UpdateConnectionInstallation`, dan `GetIndividualAccessToken` adalah izin kebijakan IAM. Mereka bukan tindakan API.

```
codeconnections:GetIndividualAccessToken
codeconnections:GetInstallationUrl
codeconnections:ListInstallationTargets
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
```

Berdasarkan ini, izin berikut diperlukan untuk menggunakan, membuat, memperbarui, atau menghapus koneksi di konsol.

```
codeconnections:CreateConnection
codeconnections>DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
codeconnections:UseConnection
codeconnections:ListInstallationTargets
codeconnections:GetInstallationUrl
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
codeconnections:GetIndividualAccessToken
```

AWS CodeConnections izin yang diperlukan untuk tindakan untuk menyelesaikan koneksi

GetIndividualAccessToken

Tindakan: `codeconnections:GetIndividualAccessToken`

Diperlukan untuk menggunakan konsol untuk menyelesaikan koneksi. Ini adalah izin kebijakan IAM saja, bukan tindakan API.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

GetInstallationUrl

Tindakan: `codeconnections:GetInstallationUrl`

Diperlukan untuk menggunakan konsol untuk menyelesaikan koneksi. Ini adalah izin kebijakan IAM saja, bukan tindakan API.

Resource:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

ListInstallationTargets

Tindakan: codeconnections:ListInstallationTargets

Diperlukan untuk menggunakan konsol untuk menyelesaikan koneksi. Ini adalah izin kebijakan IAM saja, bukan tindakan API.

Resource:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

Mulai OAuth Jabat Tangan

Tindakan: codeconnections:StartOAuthHandshake

Diperlukan untuk menggunakan konsol untuk menyelesaikan koneksi. Ini adalah izin kebijakan IAM saja, bukan tindakan API.

Resource:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

UpdateConnectionInstallation

Tindakan: codeconnections:UpdateConnectionInstallation

Diperlukan untuk menggunakan konsol untuk menyelesaikan koneksi. Ini adalah izin kebijakan IAM saja, bukan tindakan API.

Resource:arn:aws:codeconnections:*region*:*account-id*:connection/*connection-id*

Operasi ini mendukung kunci kondisi berikut.

Tindakan	Kunci kondisi
codeconnections:GetIndividualAccessToken	codeconnections:ProviderType
codeconnections:GetInstallationUrl	codeconnections:ProviderType

Tindakan	Kunci kondisi
<code>codeconnections:ListInstallationTargets</code>	N/A
<code>codeconnections:StartOAuthHandshake</code>	<code>codeconnections:ProviderType</code>
<code>codeconnections:UpdateConnectionInstallation</code>	<code>codeconnections:InstallationId</code>

Izin untuk menyiapkan host

Peran atau pengguna yang ditunjuk untuk mengelola koneksi di konsol harus memiliki izin yang diperlukan untuk mengatur host di konsol, yang mencakup otorisasi handshake ke penyedia dan menginstal aplikasi host. Gunakan izin berikut selain izin untuk host di atas.

Operasi IAM berikut digunakan oleh konsol saat melakukan pendaftaran host berbasis browser. `RegisterAppCode` dan `StartAppRegistrationHandshake` adalah izin kebijakan IAM. Mereka bukan tindakan API.

```
codeconnections:RegisterAppCode
codeconnections:StartAppRegistrationHandshake
```

Berdasarkan ini, izin berikut diperlukan untuk menggunakan, membuat, memperbarui, atau menghapus koneksi di konsol yang memerlukan host (seperti jenis penyedia yang diinstal).

```
codeconnections>CreateConnection
codeconnections>DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
codeconnections:UseConnection
codeconnections:ListInstallationTargets
codeconnections:GetInstallationUrl
codeconnections:StartOAuthHandshake
codeconnections:UpdateConnectionInstallation
codeconnections:GetIndividualAccessToken
codeconnections:RegisterAppCode
```

```
codeconnections:StartAppRegistrationHandshake
```

AWS CodeConnections izin yang diperlukan untuk tindakan untuk menyelesaikan penyiapan host

RegisterAppCode

Tindakan: `codeconnections:RegisterAppCode`

Diperlukan untuk menggunakan konsol untuk menyelesaikan pengaturan host. Ini adalah izin kebijakan IAM saja, bukan tindakan API.

Resource: `arn:aws:codeconnections:region:account-id:host/host-id`

StartAppRegistrationHandshake

Tindakan: `codeconnections:StartAppRegistrationHandshake`

Diperlukan untuk menggunakan konsol untuk menyelesaikan pengaturan host. Ini adalah izin kebijakan IAM saja, bukan tindakan API.

Resource: `arn:aws:codeconnections:region:account-id:host/host-id`

Operasi ini mendukung kunci kondisi berikut.

Melewati koneksi ke layanan

Ketika koneksi dilewatkan ke layanan (misalnya, ketika ARN koneksi disediakan dalam definisi alur untuk membuat atau memperbarui alur) pengguna harus memiliki izin `codeconnections:PassConnection`.

AWS CodeConnections izin yang diperlukan untuk meneruskan koneksi

PassConnection

Tindakan: `codeconnections:PassConnection`

Diperlukan untuk meneruskan koneksi ke layanan.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

Operasi ini juga mendukung kunci kondisi berikut:

- `codeconnections:PassedToService`

Nilai yang didukung untuk kunci kondisi

Kunci	Penyedia tindakan yang valid
<code>codeconnections:PassedToService</code>	<ul style="list-style-type: none"> • <code>codeguru-reviewer</code> • <code>codepipeline.amazonaws.com</code> • <code>proton.amazonaws.com</code>

Menggunakan koneksi

Ketika layanan seperti CodePipeline menggunakan koneksi, peran layanan harus memiliki `codeconnections:UseConnection` izin untuk koneksi tertentu.

Untuk mengelola koneksi di konsol, kebijakan pengguna harus memiliki izin `codeconnections:UseConnection`.

AWS CodeConnections tindakan yang diperlukan untuk menggunakan koneksi

UseConnection

Tindakan: `codeconnections:UseConnection`

Diperlukan untuk menggunakan koneksi.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

Operasi ini juga mendukung kunci syarat berikut:

- `codeconnections:BranchName`
- `codeconnections:FullRepositoryId`
- `codeconnections:OwnerId`
- `codeconnections:ProviderAction`
- `codeconnections:ProviderPermissionsRequired`
- `codeconnections:RepositoryName`

Nilai yang didukung untuk kunci kondisi

Kunci	Penyedia tindakan yang valid
<code>codeconnections:FullRepositoryId</code>	Nama pengguna dan nama repositori repositori, seperti <code>my-owner/my-repository</code> Didukung hanya bila koneksi sedang digunakan untuk mengakses repositori tertentu.
<code>codeconnections:ProviderPermissionsRequired</code>	<code>read_only</code> atau <code>read_write</code>
<code>codeconnections:ProviderAction</code>	<code>GetBranch</code> , <code>ListRepositories</code> , <code>ListOwners</code> , <code>ListBranches</code> , <code>StartUploadArchiveToS3</code> , <code>GitPush</code> , <code>GitPull</code> , <code>GetUploadArchiveToS3Status</code> , <code>CreatePullRequestDiffComment</code> , <code>GetPullRequest</code> , <code>ListBranchCommits</code> , <code>ListCommitFiles</code> , <code>ListPullRequestComments</code> , <code>ListPullRequestCommits</code> . Untuk informasi, lihat bagian selanjutnya.

Kunci syarat yang diperlukan untuk beberapa fungsionalitas mungkin berubah dari waktu ke waktu. Kami menyarankan agar Anda menggunakan `codeconnections:UseConnection` untuk mengontrol akses ke koneksi kecuali persyaratan kontrol akses Anda memerlukan izin yang berbeda.

Jenis akses yang didukung untuk **ProviderAction**

Ketika koneksi digunakan oleh AWS layanan, itu menghasilkan panggilan API yang dilakukan ke penyedia kode sumber Anda. Sebagai contoh, layanan mungkin mencantumkan repositori untuk koneksi Bitbucket dengan memanggil API `https://api.bitbucket.org/2.0/repositories/username`.

Kunci `ProviderAction` kondisi memungkinkan Anda untuk membatasi penyedia mana APIs yang dapat dipanggil. Karena jalur API mungkin dihasilkan secara dinamis, dan jalur bervariasi dari penyedia ke penyedia, nilai `ProviderAction` dipetakan ke nama tindakan abstrak bukan URL API.

Hal ini memungkinkan Anda untuk menulis kebijakan yang memiliki efek yang sama terlepas dari jenis penyedia untuk koneksi.

Berikut ini adalah jenis akses yang diberikan untuk masing-masing nilai `ProviderAction` yang didukung. Berikut ini adalah izin kebijakan IAM. Mereka bukan tindakan API.

AWS CodeConnections jenis akses yang didukung untuk **ProviderAction**

GetBranch

Tindakan: `codeconnections:GetBranch`

Diperlukan untuk mengakses informasi tentang cabang, seperti komit terbaru untuk cabang tersebut.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

ListRepositories

Tindakan: `codeconnections>ListRepositories`

Diperlukan untuk mengakses daftar repositori publik dan privat, termasuk detail tentang repositori tersebut, yang menjadi milik pemilik.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

ListOwners

Tindakan: `codeconnections>ListOwners`

Diperlukan untuk mengakses daftar pemilik yang memiliki akses ke koneksi.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

ListBranches

Tindakan: `codeconnections>ListBranches`

Diperlukan untuk mengakses daftar cabang yang ada pada repositori yang diberikan.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

StartUploadArchiveToS3

Tindakan: `codeconnections:StartUploadArchiveToS3`

Diperlukan untuk membaca kode sumber dan mengunggahnya ke Amazon S3.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

GitPush

Tindakan: `codeconnections:GitPush`

Diperlukan untuk menulis ke repositori menggunakan Git.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

GitPull

Tindakan: `codeconnections:GitPull`

Diperlukan untuk membaca dari repositori menggunakan Git.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

GetUploadArchiveToStatus S3

Tindakan: `codeconnections:GetUploadArchiveToS3Status`

Diperlukan untuk mengakses status pengunggahan, termasuk pesan kesalahan, yang dimulai dengan `StartUploadArchiveToS3`.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

CreatePullRequestDiffComment

Tindakan: `codeconnections>CreatePullRequestDiffComment`

Diperlukan untuk mengakses komentar pada permintaan tarik.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

GetPullRequest

Tindakan: `codeconnections:GetPullRequest`

Diperlukan untuk melihat permintaan tarik untuk repositori.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

ListBranchCommits

Tindakan: `codeconnections>ListBranchCommits`

Diperlukan untuk melihat daftar komit untuk cabang repositori.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

ListCommitFiles

Tindakan: `codeconnections>ListCommitFiles`

Diperlukan untuk melihat daftar file untuk komit.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

ListPullRequestComments

Tindakan: `codeconnections>ListPullRequestComments`

Diperlukan untuk melihat daftar komentar untuk permintaan tarik.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

ListPullRequestCommits

Tindakan: `codeconnections>ListPullRequestCommits`

Diperlukan untuk melihat daftar komit untuk permintaan tarik.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`

Izin yang didukung untuk menandai sumber daya koneksi

Operasi IAM berikut digunakan ketika penandaan sumber daya koneksi.

```
codeconnections:ListTagsForResource
codeconnections:TagResource
codeconnections:UntagResource
```

AWS CodeConnections tindakan yang diperlukan untuk menandai sumber daya koneksi

ListTagsForResource

Tindakan: `codeconnections:ListTagsForResource`

Diperlukan untuk melihat daftar tanda yang terkait dengan sumber daya koneksi.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`, `arn:aws:codeconnections:region:account-id:host/host-id`

TagResource

Tindakan: `codeconnections:TagResource`

Diperlukan untuk menandai sumber daya koneksi.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`, `arn:aws:codeconnections:region:account-id:host/host-id`

UntagResource

Tindakan: `codeconnections:UntagResource`

Diperlukan untuk menghapus tanda dari sumber daya koneksi.

Resource: `arn:aws:codeconnections:region:account-id:connection/connection-id`, `arn:aws:codeconnections:region:account-id:host/host-id`

Melewati koneksi ke tautan repositori

Ketika `repository-link` disediakan dalam konfigurasi sinkronisasi, pengguna harus memiliki `codeconnections:PassRepository` izin untuk `repository-link` ARN/resource.

AWS CodeConnections izin yang diperlukan untuk meneruskan koneksi

PassRepository

Tindakan: `codeconnections:PassRepository`

Diperlukan untuk meneruskan tautan repositori ke konfigurasi sinkronisasi.

Resource: `arn:aws:codeconnections:region:account-id:repository-link/repository-link-id`

Operasi ini juga mendukung kunci kondisi berikut:

- `codeconnections:PassedToService`

Nilai yang didukung untuk kunci kondisi

Kunci	Penyedia tindakan yang valid
<code>codeconnections:PassedToService</code>	<ul style="list-style-type: none"> • <code>cloudformation.sync.codeconnections.amazonaws.com</code>

Kunci kondisi yang didukung untuk tautan repositori

Operasi untuk tautan repositori dan sumber daya konfigurasi sinkronisasi didukung oleh kunci kondisi berikut:

- `codeconnections:Branch`

Memfilter akses dengan nama cabang yang diteruskan dalam permintaan.

Tindakan yang didukung untuk kunci kondisi

Key	Nilai valid
<code>codeconnections:Branch</code>	<p>Tindakan berikut didukung untuk kunci kondisi ini:</p> <ul style="list-style-type: none"> • <code>CreateSyncConfiguration</code>

Key	Nilai valid
	<ul style="list-style-type: none"> • UpdateSyncConfiguration • GetRepositorySyncStatus

Izin yang didukung untuk berbagi koneksi

Operasi IAM berikut digunakan saat berbagi koneksi.

```
codeconnections:GetResourcePolicy
```

AWS CodeConnections tindakan yang diperlukan untuk berbagi koneksi

GetResourcePolicy

Tindakan: `codeconnections:GetResourcePolicy`

Diperlukan untuk mengakses informasi tentang kebijakan sumber daya.

Sumber Daya: `arn:aws:codeconnections:region:account-id:connection/connection-id`

Untuk informasi selengkapnya tentang berbagi koneksi, lihat [Berbagi koneksi dengan Akun AWS](#).

Contoh kebijakan berbasis identitas

Secara default, pengguna dan peran IAM yang memiliki salah satu kebijakan terkelola untuk AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, atau AWS CodePipeline diterapkan memiliki izin untuk koneksi, notifikasi, dan aturan notifikasi yang selaras dengan maksud kebijakan tersebut. Misalnya, pengguna IAM atau peran yang memiliki salah satu kebijakan akses penuh (AWSCodeCommitFullAccess, AWSCodeBuildAdminAccessAWSCodeDeployFullAccess, atau AWSCodePipeline_FullAccess) yang diterapkan pada mereka juga memiliki akses penuh ke pemberitahuan dan aturan pemberitahuan yang dibuat untuk sumber daya untuk layanan tersebut.

Pengguna dan peran IAM lainnya tidak memiliki izin untuk membuat atau memodifikasi AWS CodeStar Pemberitahuan dan AWS CodeConnections sumber daya. Mereka juga tidak dapat melakukan tugas menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberi izin kepada pengguna dan peran untuk melakukan

operasi API pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Izin dan contoh untuk Pemberitahuan AWS CodeStar

Pernyataan dan contoh kebijakan berikut dapat membantu Anda mengelola AWS CodeStar Pemberitahuan.

Izin yang terkait dengan notifikasi dalam kebijakan terkelola akses penuh

Kebijakan `AWSCodeCommitFullAccess`, `AWSCodeBuildAdminAccess`, `AWSCodeDeployFullAccess`, dan `AWSCodePipeline_FullAccess` terkelola menyertakan pernyataan berikut untuk mengizinkan akses penuh ke notifikasi di konsol Alat Pengembang. Pengguna dengan salah satu kebijakan terkelola yang diterapkan ini juga dapat membuat dan mengelola topik Amazon SNS untuk notifikasi, berlangganan dan berhenti berlangganan pengguna ke topik, dan daftar topik untuk dipilih sebagai target untuk aturan notifikasi.

Note

Dalam kebijakan dikelola, kunci syarat `codestar-notifications:NotificationsForResource` akan memiliki nilai khusus untuk jenis sumber daya untuk layanan. Misalnya, dalam kebijakan akses penuh untuk `CodeCommit`, nilainya adalah `arn:aws:codecommit:*`.

```
{
  "Sid": "CodeStarNotificationsReadWriteAccess",
  "Effect": "Allow",
  "Action": [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {"codestar-notifications:NotificationsForResource" :
      "arn:aws:<vendor-code>:*"}
  }
}
```

```

},
{
  "Sid": "CodeStarNotificationsListAccess",
  "Effect": "Allow",
  "Action": [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsForResource",
    "codestar-notifications:ListEventTypes"
  ],
  "Resource": "*"
},
{
  "Sid": "CodeStarNotificationsSNSTopicCreateAccess",
  "Effect": "Allow",
  "Action": [
    "sns:CreateTopic",
    "sns:SetTopicAttributes"
  ],
  "Resource": "arn:aws:sns:*:*:codestar-notifications*"
},
{
  "Sid": "SNSTopicListAccess",
  "Effect": "Allow",
  "Action": [
    "sns:ListTopics"
  ],
  "Resource": "*"
},
{
  "Sid": "CodeStarNotificationsChatbotAccess",
  "Effect": "Allow",
  "Action": [
    "chatbot:DescribeSlackChannelConfigurations",
    "chatbot:ListMicrosoftTeamsChannelConfigurations"
  ],
  "Resource": "*"
}

```

Izin yang terkait dengan notifikasi dalam kebijakan terkelola hanya-baca

Kebijakan `AWSCodeCommitReadOnlyAccess`,
`AWSCodeBuildReadOnlyAccess` `AWSCodeDeployReadOnlyAccess`, dan

AWSCodePipeline_ReadOnlyAccesssterkelola menyertakan pernyataan berikut untuk mengizinkan akses hanya-baca ke notifikasi. Misalnya, mereka dapat melihat notifikasi untuk sumber daya di konsol Alat Developer, tetapi tidak dapat membuat, mengelola, atau berlangganan notifikasi.

Note

Dalam kebijakan dikelola, kunci syarat `codestar-notifications:NotificationsForResource` akan memiliki nilai khusus untuk jenis sumber daya untuk layanan. Misalnya, dalam kebijakan akses penuh untuk CodeCommit, nilainya adalah `arn:aws:codecommit:*`.

```
{
  "Sid": "CodeStarNotificationsPowerUserAccess",
  "Effect": "Allow",
  "Action": [
    "codestar-notifications:DescribeNotificationRule"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
  }
},
{
  "Sid": "CodeStarNotificationsListAccess",
  "Effect": "Allow",
  "Action": [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListEventTypes",
    "codestar-notifications:ListTargets"
  ],
  "Resource": "*"
}
```

Izin terkait notifikasi dalam kebijakan terkelola lainnya

Kebijakan `AWSCodeCommitPowerUser`, `AWSCodeBuildDeveloperAccess`, dan `AWSCodeBuildDeveloperAccesssterkelola` mencakup pernyataan berikut untuk mengizinkan pengembang menggunakan salah satu kebijakan terkelola ini yang diterapkan untuk membuat,

mengedit, dan berlangganan notifikasi. Mereka tidak dapat menghapus aturan notifikasi atau mengelola tanda untuk sumber daya.

Note

Dalam kebijakan dikelola, kunci syarat `codestar-notifications:NotificationsForResource` akan memiliki nilai khusus untuk jenis sumber daya untuk layanan. Misalnya, dalam kebijakan akses penuh untuk CodeCommit, nilainya adalah `arn:aws:codecommit:*`.

```
{
  "Sid": "CodeStarNotificationsReadWriteAccess",
  "Effect": "Allow",
  "Action": [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {"codestar-notifications:NotificationsForResource" :
"arn:aws:<vendor-code>:*"}
  }
},
{
  "Sid": "CodeStarNotificationsListAccess",
  "Effect": "Allow",
  "Action": [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsForResource",
    "codestar-notifications:ListEventTypes"
  ],
  "Resource": "*"
},
{
  "Sid": "SNSTopicListAccess",
  "Effect": "Allow",
  "Action": [
```

```
        "sns:ListTopics"
    ],
    "Resource": "*"
  },
  {
    "Sid": "CodeStarNotificationsChatbotAccess",
    "Effect": "Allow",
    "Action": [
      "chatbot:DescribeSlackChannelConfigurations",
      "chatbot:ListMicrosoftTeamsChannelConfigurations"
    ],
    "Resource": "*"
  }
}
```

Contoh: Kebijakan tingkat administrator untuk mengelola Pemberitahuan AWS CodeStar

Dalam contoh ini, Anda ingin memberi pengguna IAM di AWS akun Anda akses penuh ke AWS CodeStar Notifikasi sehingga pengguna dapat meninjau detail aturan notifikasi dan daftar aturan pemberitahuan, target, dan jenis acara. Anda juga ingin mengizinkan pengguna untuk menambahkan, memperbarui, dan menghapus aturan notifikasi. Ini adalah kebijakan akses penuh, setara dengan izin pemberitahuan yang disertakan sebagai bagian dari `AWSCodeBuildAdminAccess`, `AWSCodeCommitFullAccess`, `AWSCodeDeployFullAccess`, dan kebijakan `AWSCodePipeline_FullAccess` terkelola. Seperti kebijakan terkelola tersebut, Anda hanya boleh melampirkan pernyataan kebijakan semacam ini ke pengguna, grup, atau peran IAM yang memerlukan akses administratif penuh ke pemberitahuan dan aturan notifikasi di seluruh AWS akun Anda.

Note


Kebijakan ini berisi izin `CreateNotificationRule`. Setiap pengguna dengan kebijakan ini yang diterapkan pada pengguna atau peran IAM mereka akan dapat membuat aturan pemberitahuan untuk setiap dan semua jenis sumber daya yang didukung oleh AWS CodeStar Pemberitahuan di AWS akun, bahkan jika pengguna tersebut tidak memiliki akses ke sumber daya itu sendiri. Misalnya, pengguna dengan kebijakan ini dapat membuat aturan notifikasi untuk CodeCommit repositori tanpa izin untuk mengaksesnya sendiri. CodeCommit

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCodeStarNotificationsFullAccess",
      "Effect": "Allow",
      "Action": [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications>DeleteNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe",
        "codestar-notifications>DeleteTarget",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsForResource",
        "codestar-notifications:TagResource",
        "codestar-notifications:UntagResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Contoh: Kebijakan tingkat kontributor untuk menggunakan Notifikasi AWS CodeStar

Dalam contoh ini, Anda ingin memberikan akses ke day-to-day penggunaan AWS CodeStar Notifikasi, seperti membuat dan berlangganan notifikasi, tetapi tidak untuk tindakan yang lebih merusak, seperti menghapus aturan atau target notifikasi. Ini setara dengan akses yang disediakan dalam `AWSCodeBuildDeveloperAccess`, `AWSCodeDeployDeveloperAccess`, dan kebijakan `AWSCodeCommitPowerUser` terkelola.

 Note

Kebijakan ini berisi izin `CreateNotificationRule`. Setiap pengguna dengan kebijakan ini yang diterapkan pada pengguna atau peran IAM mereka akan dapat membuat aturan pemberitahuan untuk setiap dan semua jenis sumber daya yang didukung oleh AWS

CodeStar Pemberitahuan di AWS akun, bahkan jika pengguna tersebut tidak memiliki akses ke sumber daya itu sendiri. Misalnya, pengguna dengan kebijakan ini dapat membuat aturan notifikasi untuk CodeCommit repositori tanpa izin untuk mengaksesnya sendiri. CodeCommit

```
{
  "Version": "2012-10-17",
  "Sid": "AWSCodeStarNotificationsPowerUserAccess",
  "Effect": "Allow",
  "Action": [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsForResource"
  ],
  "Resource": "*"
}
```

Contoh: read-only-level Kebijakan untuk menggunakan AWS CodeStar Notifikasi

Dalam contoh ini, Anda ingin memberi pengguna IAM di akun Anda akses hanya baca ke aturan notifikasi, target, dan jenis peristiwa di akun AWS Anda. Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang memungkinkan melihat item ini. Ini setara dengan izin yang disertakan sebagai bagian dari `AWSCodeBuildReadOnlyAccess`, `AWSCodeCommitReadOnly`, dan kebijakan `AWSCodePipeline_ReadOnlyAccesssterkelola`.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "CodeNotificationforReadOnly",
  "Statement": [
    {
      "Sid": "ReadsAccess",
```

```

    "Effect": "Allow",
    "Action": [
      "codestar-notifications:DescribeNotificationRule",
      "codestar-notifications:ListNotificationRules",
      "codestar-notifications:ListTargets",
      "codestar-notifications:ListEventTypes"
    ],
    "Resource": "*"
  }
]
}

```

Izin dan contoh untuk AWS CodeConnections

Pernyataan dan contoh kebijakan berikut dapat membantu Anda mengelola AWS CodeConnections.

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

Contoh: Kebijakan untuk membuat AWS CodeConnections dengan CLI dan melihat dengan konsol

Peran atau pengguna yang ditunjuk untuk menggunakan AWS CLI atau SDK untuk melihat, membuat, menandai, atau menghapus koneksi harus memiliki izin terbatas pada hal berikut.

Note

Anda tidak dapat menyelesaikan koneksi di konsol dengan hanya izin berikut. Anda perlu menambahkan izin di bagian berikutnya.

Untuk menggunakan konsol untuk melihat daftar koneksi yang tersedia, melihat tanda, dan menggunakan koneksi, gunakan kebijakan berikut.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConnectionsFullAccess",
      "Effect": "Allow",

```

```
"Action": [  
  "codeconnections:CreateConnection",  
  "codeconnections>DeleteConnection",  
  "codeconnections:UseConnection",  
  "codeconnections:GetConnection",  
  "codeconnections:ListConnections",  
  "codeconnections:TagResource",  
  "codeconnections:ListTagsForResource",  
  "codeconnections:UntagResource"  
],  
"Resource": "*" ]  
}
```

Contoh: Kebijakan untuk membuat AWS CodeConnections dengan konsol

Peran atau pengguna yang ditunjuk untuk mengelola koneksi di konsol harus memiliki izin yang diperlukan untuk menyelesaikan koneksi di konsol dan membuat instalasi, yang mencakup otorisasi handshake ke penyedia dan membuat instalasi untuk koneksi untuk digunakan. `UseConnection` juga harus ditambahkan untuk menggunakan koneksi di konsol. Gunakan kebijakan berikut untuk melihat, menggunakan, membuat, menandai, atau menghapus koneksi di konsol.

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan `codeconnections` ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Note

Untuk sumber daya yang dibuat menggunakan konsol, tindakan pernyataan kebijakan harus disertakan `codestar-connections` sebagai awalan layanan seperti yang ditunjukkan pada contoh berikut.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "codestar-connections:CreateConnection",
      "codestar-connections>DeleteConnection",
      "codestar-connections:GetConnection",
      "codestar-connections:ListConnections",
      "codestar-connections:GetInstallationUrl",
      "codestar-connections:GetIndividualAccessToken",
      "codestar-connections:ListInstallationTargets",
      "codestar-connections:StartOAuthHandshake",
      "codestar-connections:UpdateConnectionInstallation",
      "codestar-connections:UseConnection",
      "codestar-connections:TagResource",
      "codestar-connections:ListTagsForResource",
      "codestar-connections:UntagResource"
    ],
    "Resource": [
      "*"
    ]
  }
]
}

```

Contoh: Kebijakan tingkat administrator untuk mengelola AWS CodeConnections

Dalam contoh ini, Anda ingin memberikan pengguna IAM di AWS akun Anda akses penuh CodeConnections sehingga pengguna dapat menambah, memperbarui, dan menghapus koneksi. Ini adalah kebijakan akses penuh, setara dengan kebijakan yang `AWSCodePipeline_FullAccess` dikelola. Seperti kebijakan terkelola tersebut, Anda hanya boleh melampirkan pernyataan kebijakan semacam ini ke pengguna, grup, atau peran IAM yang memerlukan akses administratif penuh ke koneksi di seluruh AWS akun Anda.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "ConnectionsFullAccess",
    "Effect": "Allow",
    "Action": [
        "codeconnections:CreateConnection",
        "codeconnections>DeleteConnection",
        "codeconnections:UseConnection",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListInstallationTargets",
        "codeconnections:GetInstallationUrl",
        "codeconnections:StartOAuthHandshake",
        "codeconnections:UpdateConnectionInstallation",
        "codeconnections:GetIndividualAccessToken",
        "codeconnections:TagResource",
        "codeconnections:ListTagsForResource",
        "codeconnections:UntagResource"
    ],
    "Resource": "*"
}
]
}

```

Contoh: Kebijakan tingkat kontributor untuk menggunakan AWS CodeConnections

Dalam contoh ini, Anda ingin memberikan akses ke day-to-day penggunaan CodeConnections, seperti membuat dan melihat detail koneksi, tetapi tidak untuk tindakan yang lebih merusak, seperti menghapus koneksi.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCodeConnectionsPowerUserAccess",
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateConnection",
        "codeconnections:UseConnection",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",

```

```

        "codeconnections:ListInstallationTargets",
        "codeconnections:GetInstallationUrl",
        "codeconnections:GetIndividualAccessToken",
        "codeconnections:StartOAuthHandshake",
        "codeconnections:UpdateConnectionInstallation",
        "codeconnections:ListTagsForResource"
    ],
    "Resource": "*"
}
]
}

```

Contoh: read-only-level Kebijakan untuk menggunakan AWS CodeConnections

Dalam contoh ini, Anda ingin memberikan pengguna IAM di akun Anda akses hanya-baca ke koneksi di akun Anda. AWS Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang memungkinkan melihat item ini.

JSON

```

{
  "Version": "2012-10-17",
  "Id": "ConnectionsforReadOnly",
  "Statement": [
    {
      "Sid": "ReadsAPIAccess",
      "Effect": "Allow",
      "Action": [
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListInstallationTargets",
        "codeconnections:GetInstallationUrl",
        "codeconnections:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}

```

Contoh: Batasi izin VPC host menggunakan tombol konteks VpcId

Dalam contoh berikut, pelanggan dapat menggunakan kunci VpcIdkonteks untuk membatasi pembuatan atau pengelolaan host ke host dengan VPC tertentu.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateHost",
        "codeconnections:UpdateHost"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "codeconnections:VpcId": "vpc-EXAMPLE"
        }
      }
    }
  ]
}
```

Menggunakan tag untuk mengontrol akses ke AWS CodeConnections sumber daya

Tag dapat dilampirkan ke sumber daya atau diteruskan atas permintaan ke layanan yang mendukung penandaan. Di AWS CodeConnections, sumber daya dapat memiliki tag, dan beberapa tindakan dapat menyertakan tag. Saat membuat kebijakan IAM, Anda dapat menggunakan kunci syarat tanda berikut:

- Manakah pengguna yang dapat melakukan tindakan pada sumber daya alur, berdasarkan tanda yang telah dimiliki.
- Tanda apa yang dapat diteruskan dalam permintaan tindakan.
- Apakah kunci tanda tertentu dapat digunakan dalam permintaan.

Contoh berikut menunjukkan cara menentukan kondisi tag dalam kebijakan untuk AWS CodeConnections pengguna.

Example 1: Izinkan tindakan berdasarkan tanda dalam permintaan

Kebijakan berikut memberikan izin kepada pengguna untuk membuat koneksi. AWS CodeConnections

Untuk melakukan itu, memungkinkan tindakan `CreateConnection` dan `TagResource` jika permintaan menentukan tag bernama `Project` dengan nilai `ProjectA`. (Kunci syarat `aws:RequestTag` digunakan untuk mengontrol tanda yang dapat dilewatkan dalam permintaan IAM.) Syarat `aws:TagKeys` memastikan sensitivitas kasus kunci tanda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateConnection",
        "codeconnections:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Example 2: Izinkan tindakan berdasarkan tanda sumber daya

Kebijakan berikut memberi pengguna izin untuk melakukan tindakan pada, dan mendapatkan informasi tentang, sumber daya di AWS CodeConnections.

Untuk melakukan itu, memungkinkan tindakan tertentu jika alur memiliki tanda bernama `Project` dengan nilai `ProjectA`. (Kunci syarat `aws:RequestTag` digunakan untuk mengontrol tanda yang dapat dilewatkan dalam permintaan IAM.) Syarat `aws:TagKeys` memastikan kunci tanda peka huruf besar dan kecil.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codeconnections:CreateConnection",
        "codeconnections>DeleteConnection",
        "codeconnections:ListConnections"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "ProjectA"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Project"]
        }
      }
    }
  ]
}
```

Menggunakan notifikasi dan koneksi di konsol

Pengalaman notifikasi dibangun ke dalam CodeBuild, CodeCommit, CodeDeploy, dan CodePipeline konsol, serta di konsol Alat Pengembang di bilah navigasi Pengaturan itu sendiri. Untuk mengakses notifikasi di konsol, Anda harus memiliki salah satu kebijakan terkelola untuk layanan tersebut diterapkan, atau Anda harus memiliki seperangkat izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AWS CodeStar Pemberitahuan dan AWS CodeConnections sumber daya di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi

sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut. Untuk informasi selengkapnya tentang pemberian akses ke AWS CodeBuild AWS CodeCommit, AWS CodeDeploy,, dan AWS CodePipeline, termasuk akses ke konsol tersebut, lihat topik berikut:

- CodeBuild: [Menggunakan kebijakan berbasis identitas](#) untuk CodeBuild
- CodeCommit: [Menggunakan kebijakan berbasis identitas](#) untuk CodeCommit
- AWS CodeDeploy: [Identitas dan manajemen akses untuk AWS CodeDeploy](#)
- CodePipeline: [Kontrol akses dengan kebijakan IAM](#)

AWS CodeStar Pemberitahuan tidak memiliki kebijakan AWS terkelola. Untuk menyediakan akses ke fungsionalitas notifikasi, Anda harus menerapkan salah satu kebijakan terkelola untuk salah satu layanan yang terdaftar sebelumnya, atau Anda harus membuat kebijakan dengan tingkat izin yang ingin Anda berikan kepada pengguna atau entitas, dan kemudian melampirkan kebijakan tersebut ke pengguna, grup, atau peran yang memerlukan izin tersebut. Untuk informasi selengkapnya dan contoh, lihat berikut ini:

- [Contoh: Kebijakan tingkat administrator untuk mengelola Pemberitahuan AWS CodeStar](#)
- [Contoh: Kebijakan tingkat kontributor untuk menggunakan Notifikasi AWS CodeStar](#)
- [Contoh: read-only-level Kebijakan untuk menggunakan AWS CodeStar Notifikasi.](#)

AWS CodeConnections tidak memiliki kebijakan AWS terkelola. Anda menggunakan izin dan kombinasi izin untuk akses, seperti izin yang dirinci. [Izin untuk menyelesaikan koneksi](#)

Untuk informasi selengkapnya, lihat berikut ini:

- [Contoh: Kebijakan tingkat administrator untuk mengelola AWS CodeConnections](#)
- [Contoh: Kebijakan tingkat kontributor untuk menggunakan AWS CodeConnections](#)
- [Contoh: read-only-level Kebijakan untuk menggunakan AWS CodeConnections](#)

Anda tidak perlu mengizinkan izin konsol untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

Pemecahan Masalah AWS CodeStar Pemberitahuan dan AWS CodeConnections identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temukan saat bekerja dengan notifikasi dan IAM.

Topik

- [Saya seorang administrator dan ingin mengizinkan orang lain mengakses notifikasi](#)
- [Saya membuat topik Amazon SNS dan menambahkannya sebagai target aturan notifikasi, tapi saya tidak menerima email tentang peristiwa](#)
- [Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses AWS CodeStar Pemberitahuan dan AWS CodeConnections sumber daya saya](#)

Saya seorang administrator dan ingin mengizinkan orang lain mengakses notifikasi

Untuk memungkinkan orang lain mengakses AWS CodeStar Notifikasi dan AWS CodeConnections, Anda harus memberikan izin kepada orang atau aplikasi yang membutuhkan akses. Jika Anda menggunakan AWS IAM Identity Center untuk mengelola orang dan aplikasi, Anda menetapkan set izin kepada pengguna atau grup untuk menentukan tingkat akses mereka. Set izin secara otomatis membuat dan menetapkan kebijakan IAM ke peran IAM yang terkait dengan orang atau aplikasi. Untuk informasi selengkapnya, lihat [Set izin](#) di Panduan AWS IAM Identity Center Pengguna.

Jika Anda tidak menggunakan IAM Identity Center, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Anda kemudian harus melampirkan kebijakan ke entitas yang memberi mereka izin yang benar dalam AWS CodeStar Pemberitahuan dan AWS CodeConnections. Setelah izin diberikan, berikan kredensialnya kepada pengguna atau pengembang aplikasi. Mereka akan menggunakan kredensial tersebut untuk mengakses AWS. Untuk mempelajari selengkapnya tentang membuat pengguna, grup, kebijakan, dan izin IAM, lihat [Identitas dan Kebijakan IAM dan izin di IAM di Panduan Pengguna IAM](#).

Untuk informasi spesifik AWS CodeStar Pemberitahuan, lihat [Izin dan contoh untuk Pemberitahuan AWS CodeStar](#).

Saya membuat topik Amazon SNS dan menambahkannya sebagai target aturan notifikasi, tapi saya tidak menerima email tentang peristiwa

Untuk menerima notifikasi tentang peristiwa, Anda harus memiliki topik Amazon SNS valid berlangganan sebagai target untuk aturan notifikasi, dan alamat email Anda harus berlangganan topik Amazon SNS. Untuk memecahkan masalah dengan topik Amazon SNS, periksa berikut ini:

- Pastikan bahwa topik Amazon SNS berada di AWS Wilayah yang sama dengan aturan notifikasi.
- Periksa untuk memastikan bahwa alias email Anda berlangganan topik yang benar, dan bahwa Anda telah mengonfirmasi langganan. Untuk informasi selengkapnya, lihat [Berlangganan titik akhir ke topik Amazon SNS](#).
- Verifikasi bahwa kebijakan topik telah dimodifikasi untuk memungkinkan AWS CodeStar Pemberitahuan mendorong pemberitahuan ke topik tersebut. Kebijakan topik harus mencakup pernyataan yang serupa dengan yang berikut ini:

```
{
  "Sid": "AWSCodeStarNotifications_publish",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "codestar-notifications.amazonaws.com"
    ]
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopicName",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012"
    }
  }
}
```

Untuk informasi selengkapnya, lihat [Pengaturan](#).

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses AWS CodeStar Pemberitahuan dan AWS CodeConnections sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang

dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah AWS CodeStar Pemberitahuan dan AWS CodeConnections mendukung fitur ini, lihat [Bagaimana fitur di konsol alat developer bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

Menggunakan peran terkait layanan untuk Pemberitahuan AWS CodeStar

AWS CodeStar Pemberitahuan menggunakan AWS Identity and Access Management peran [terkait layanan](#) (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Notifikasi. AWS CodeStar Peran terkait layanan telah ditentukan sebelumnya oleh AWS CodeStar Pemberitahuan dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda. Peran ini dibuat untuk Anda saat pertama kali Anda membuat aturan notifikasi. Anda tidak perlu membuat peran.

Peran terkait layanan membuat pengaturan AWS CodeStar Notifikasi lebih mudah karena Anda tidak perlu menambahkan izin secara manual. AWS CodeStar Notifikasi mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS CodeStar Pemberitahuan yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk menghapus peran tertaut layanan, Anda harus menghapus sumber daya terkaitnya terlebih dahulu. Ini melindungi sumber daya AWS CodeStar Pemberitahuan karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran yang terhubung dengan layanan, lihat [AWS Layanan yang Bekerja dengan IAM](#).

Izin peran terkait layanan untuk Pemberitahuan AWS CodeStar

AWS CodeStar Notifikasi menggunakan peran `AWSService RoleForCodeStarNotifications` terkait layanan untuk mengambil informasi tentang peristiwa yang terjadi di toolchain Anda dan mengirim pemberitahuan ke target yang Anda tentukan.

Peran `AWSService RoleForCodeStarNotifications` terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `codestar-notifications.amazonaws.com`

Kebijakan izin peran memungkinkan AWS CodeStar Pemberitahuan untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `PutRule` pada CloudWatch Event rules that are named `awscodestar-notifications-*`
- Tindakan: `DescribeRule` pada CloudWatch Event rules that are named `awscodestar-notifications-*`
- Tindakan: `PutTargets` pada CloudWatch Event rules that are named `awscodestar-notifications-*`
- Tindakan: `CreateTopic` ke create Amazon SNS topics for use with AWS CodeStar Notifications with the prefix `CodeStarNotifications-`
- Tindakan: `GetCommentsForPullRequests` pada all comments on all pull requests in all CodeCommit repositories in the AWS account
- Tindakan: `GetCommentsForComparedCommit` pada all comments on all commits in all CodeCommit repositories in the AWS account
- Tindakan: `GetDifferences` pada all commits in all CodeCommit repositories in the AWS account
- Tindakan: `GetCommentsForComparedCommit` pada all comments on all commits in all CodeCommit repositories in the AWS account
- Tindakan: `GetDifferences` pada all commits in all CodeCommit repositories in the AWS account

- Tindakan: DescribeSlackChannelConfigurations pada all AWS Chatbot clients in the AWS account
- Tindakan: UpdateSlackChannelConfiguration pada all AWS Chatbot clients in the AWS account
- Tindakan: ListActionExecutions pada all actions in all pipelines in the AWS account
- Tindakan: GetFile pada all files in all CodeCommit repositories in the AWS account unless otherwise tagged

Anda dapat melihat tindakan ini di pernyataan kebijakan untuk peran AWSServiceRoleForCodeStarNotifications terkait layanan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule"
      ],
      "Resource": "arn:aws:events:*:*:rule/awscodestarnotifications-*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "sns:CreateTopic"
      ],
      "Resource": "arn:aws:sns:*:*:CodeStarNotifications-*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetDifferences",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:UpdateSlackChannelConfiguration",

```

```

        "codepipeline:ListActionExecutions"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "codecommit:GetFile"
    ],
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "aws:ResourceTag/ExcludeFileContentFromNotifications": "true"
      }
    },
    "Effect": "Allow"
  }
]
}

```

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat [Izin Peran Tertaut Layanan](#) di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Pemberitahuan AWS CodeStar

Anda tidak perlu membuat peran terkait layanan secara manual. Anda dapat menggunakan konsol Alat Pengembang atau CreateNotificationRule API dari AWS CLI atau SDKs untuk membuat aturan notifikasi. Anda juga bisa langsung memanggil API secara langsung. Apa pun metode yang Anda gunakan, peran terkait layanan dibuat untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Anda dapat menggunakan konsol Alat Pengembang atau CreateNotificationRule API dari AWS CLI atau SDKs untuk membuat aturan notifikasi. Anda juga bisa langsung memanggil API secara langsung. Apa pun metode yang Anda gunakan, peran terkait layanan dibuat untuk Anda.

Mengedit peran terkait layanan untuk Pemberitahuan AWS CodeStar

Setelah membuat peran terkait layanan, Anda tidak dapat mengubah namanya karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menggunakan IAM untuk

mengedit deskripsi peran. Untuk informasi selengkapnya, lihat [Mengedit Peran yang Terhubung dengan Layanan](#) di Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Pemberitahuan AWS CodeStar

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami menyarankan Anda menghapus peran itu. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya. Untuk AWS CodeStar Pemberitahuan, ini berarti menghapus semua aturan notifikasi yang menggunakan peran layanan di AWS akun Anda.

Note

Jika layanan AWS CodeStar Notifikasi menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya AWS CodeStar Pemberitahuan yang digunakan oleh AWSService RoleForCodeStarNotifications

1. Buka konsol Alat AWS Pengembang di <https://console.aws.amazon.com/codesuite/pengaturan/pemberitahuan>.

Note

Aturan pemberitahuan berlaku untuk AWS Wilayah tempat mereka dibuat. Jika Anda memiliki aturan pemberitahuan di lebih dari satu AWS Wilayah, gunakan pemilih Wilayah untuk mengubah. Wilayah AWS

2. Pilih semua aturan notifikasi yang muncul dalam daftar, dan kemudian pilih Hapus.
3. Ulangi langkah-langkah ini di semua AWS Wilayah tempat Anda membuat aturan notifikasi.

Untuk menggunakan IAM untuk menghapus peran terkait layanan

Gunakan konsol IAM AWS CLI, atau AWS Identity and Access Management API untuk menghapus peran AWSService RoleForCodeStarNotifications terkait layanan. Untuk informasi selengkapnya, silakan lihat [Menghapus Peran Terkait Layanan](#) di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran AWS CodeStar terkait layanan Pemberitahuan

AWS CodeStar Pemberitahuan mendukung penggunaan peran terkait layanan di semua AWS Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat [AWS Wilayah dan Titik Akhir](#) dan [AWS CodeStar Pemberitahuan](#).

Menggunakan peran terkait layanan untuk AWS CodeConnections

AWS CodeConnections menggunakan AWS Identity and Access Management peran [terkait layanan](#) (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS CodeConnections Peran terkait layanan telah ditentukan sebelumnya oleh AWS CodeConnections dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda. Peran ini dibuat untuk Anda saat pertama kali Anda membuat koneksi. Anda tidak perlu membuat peran.

Peran terkait layanan membuat pengaturan AWS CodeConnections lebih mudah karena Anda tidak perlu menambahkan izin secara manual. AWS CodeConnections mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS CodeConnections dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk menghapus peran tertaut layanan, Anda harus menghapus sumber daya terkaitnya terlebih dahulu. Ini melindungi AWS CodeConnections sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran yang terhubung dengan layanan, lihat [AWS Layanan yang Bekerja dengan IAM](#).

Note

Tindakan untuk sumber daya yang dibuat di bawah awalan layanan baru codeconnections tersedia. Membuat sumber daya di bawah awalan layanan baru akan digunakan codeconnections di sumber daya ARN. Tindakan dan sumber daya untuk awalan codestar-connections layanan tetap tersedia. Saat menentukan sumber daya dalam kebijakan IAM, awalan layanan harus sesuai dengan sumber daya.

Izin peran terkait layanan untuk AWS CodeConnections

AWS CodeConnections menggunakan peran `AWSService RoleForGitSync` terkait layanan untuk menggunakan sinkronisasi Git dengan repositori berbasis Git yang terhubung.

Peran `AWSService RoleForGitSync` terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `repository.sync.codeconnections.amazonaws.com`

Kebijakan izin peran bernama `AWSGit SyncServiceRolePolicy` memungkinkan AWS CodeConnections untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: Memberikan izin untuk memungkinkan pengguna membuat koneksi ke repositori berbasis Git eksternal dan menggunakan sinkronisasi Git dengan repositori tersebut.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat [Izin Peran Tertaut Layanan](#) di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk AWS CodeConnections

Anda tidak perlu membuat peran terkait layanan secara manual. Anda membuat peran saat membuat sumber daya untuk proyek yang disinkronkan GIT dengan API. `CreateRepositoryLink`

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda.

Mengedit peran terkait layanan untuk AWS CodeConnections

Setelah membuat peran terkait layanan, Anda tidak dapat mengubah namanya karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menggunakan IAM untuk mengedit deskripsi peran. Untuk informasi selengkapnya, lihat [Mengedit Peran yang Terhubung dengan Layanan](#) di Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS CodeConnections

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami menyarankan Anda menghapus peran itu. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Anda harus membersihkan sumber

daya peran yang terhubung dengan layanan sebelum menghapusnya. Ini berarti menghapus semua koneksi yang menggunakan peran layanan di AWS akun Anda.

Note

Jika AWS CodeConnections layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus AWS CodeConnections sumber daya yang digunakan oleh AWSService RoleForGitSync

1. Buka konsol Alat Pengembang, lalu pilih Pengaturan.
2. Pilih semua koneksi yang muncul dalam daftar, lalu pilih Hapus.
3. Ulangi langkah-langkah ini di semua AWS Wilayah tempat Anda membuat koneksi.

Untuk menggunakan IAM untuk menghapus peran terkait layanan

Gunakan konsol IAM AWS CLI, atau AWS Identity and Access Management API untuk menghapus peran AWSService RoleForGitSync terkait layanan. Untuk informasi selengkapnya, silakan lihat [Menghapus Peran Terkait Layanan](#) di Panduan Pengguna IAM.

Wilayah yang didukung untuk AWS CodeConnections peran terkait layanan

AWS CodeConnections mendukung penggunaan peran terkait layanan di semua AWS Wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat [Wilayah dan Titik Akhir AWS](#).

AWS kebijakan terkelola untuk AWS CodeConnections

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

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

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

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

Note

Tindakan untuk sumber daya yang dibuat di bawah awalan layanan baru `codeconnections` tersedia. Membuat sumber daya di bawah awalan layanan baru akan digunakan `codeconnections` di sumber daya ARN. Tindakan dan sumber daya untuk awalan `codestar-connections` layanan tetap tersedia. Saat menentukan sumber daya dalam kebijakan IAM, awalan layanan harus sesuai dengan sumber daya.

AWS kebijakan terkelola: AWSGit SyncServiceRolePolicy

Anda tidak dapat melampirkan AWSGit SyncServiceRolePolicy ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan AWS CodeConnections untuk melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk AWS CodeConnections](#).

Kebijakan ini memungkinkan pelanggan untuk mengakses repositori berbasis Git untuk digunakan dengan koneksi. Pelanggan akan mengakses sumber daya ini setelah menggunakan CreateRepositoryLink API.

Detail izin

Kebijakan ini mencakup izin berikut.

- `codeconnections`— Memberikan izin untuk memungkinkan pengguna membuat koneksi ke repositori berbasis Git eksternal.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessGitRepos",
      "Effect": "Allow",
      "Action": [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource": [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

AWS CodeConnections pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS CodeConnections sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman [Riwayat AWS CodeConnections dokumen](#).

Ubah	Deskripsi	Date
AWSGitSyncServiceRolePolicy — Kebijakan yang diperbarui	Nama layanan AWS CodeStar Connections diubah menjadi AWS CodeConnections. Memperbarui kebijakan untuk	April 26, 2024

Ubah	Deskripsi	Date
	sumber daya ARNs yang berisi kedua awalan layanan.	
AWSGitSyncServiceRolePolicy – Kebijakan baru	AWS CodeStar Connections menambahkan kebijakan. Memberikan izin untuk memungkinkan pengguna koneksi menggunakan sinkronisasi Git dengan repositori berbasis Git yang terhubung.	26 November 2023
AWS CodeConnections mulai melacak perubahan	AWS CodeConnections mulai melacak perubahan untuk kebijakan yang AWS dikelola.	26 November 2023

Validasi kepatuhan untuk AWS CodeStar Pemberitahuan dan AWS CodeConnections

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat [AWS layanan dalam lingkup oleh program kepatuhan](#). Untuk informasi umum, lihat [Program kepatuhan AWS](#).

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

Tanggung jawab kepatuhan Anda saat menggunakan AWS CodeStar Pemberitahuan dan AWS CodeConnections ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta 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 yang berfokus pada keamanan dan kepatuhan. AWS

- [AWS sumber daya kepatuhan](#) - Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Config](#) AWS Layanan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub CSPM](#)— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan dalam AWS CodeStar Pemberitahuan dan AWS CodeConnections

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat [infrastruktur AWS global](#).

- Aturan pemberitahuan khusus untuk Wilayah AWS tempat pembuatannya. Jika Anda memiliki aturan notifikasi di lebih dari satu Wilayah AWS, gunakan pemilih Wilayah untuk meninjau aturan notifikasi di masing-masing Wilayah AWS aturan.
- AWS CodeStar Notifikasi bergantung pada topik Amazon Simple Notification Service (Amazon SNS) sebagai target aturan notifikasi. Informasi tentang topik Amazon SNS dan target aturan notifikasi mungkin disimpan di Wilayah AWS yang berbeda dari Wilayah di mana Anda mengonfigurasi aturan notifikasi.

Keamanan infrastruktur dalam AWS CodeStar Pemberitahuan dan AWS CodeConnections

Sebagai fitur dalam layanan terkelola, AWS CodeStar Pemberitahuan dan AWS CodeConnections dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam [Amazon Web Services: Ringkasan proses keamanan](#) whitepaper.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS CodeStar Notifikasi dan AWS CodeConnections melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.0 atau versi yang lebih baru. Klien juga harus support suite cipher dengan Perfect Forward Secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern mendukung mode ini.

Permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara untuk menandatangani permintaan.

Lalu lintas antar AWS CodeConnections sumber daya lintas Wilayah

Jika Anda menggunakan fitur koneksi untuk mengaktifkan koneksi sumber daya Anda, Anda menyetujui dan menginstruksikan kami untuk menyimpan dan memproses informasi yang terkait dengan sumber daya koneksi tersebut di Wilayah AWS luar Wilayah AWS tempat Anda menggunakan layanan yang mendasarinya, semata-mata sehubungan dengan, dan untuk tujuan tunggal, menyediakan koneksi ke sumber daya tersebut di Wilayah selain tempat sumber daya dibuat.

Untuk informasi selengkapnya, lihat [Sumber daya global di AWS CodeConnections](#).

Note

Jika Anda menggunakan fitur koneksi untuk mengaktifkan koneksi sumber daya Anda di Wilayah yang tidak perlu diaktifkan terlebih dahulu, kami akan menyimpan dan memproses informasi sebagaimana dirinci dalam topik sebelumnya.

Untuk koneksi yang dibuat di Wilayah yang harus diaktifkan terlebih dahulu, seperti Wilayah Eropa (Milan), kami hanya akan menyimpan dan memproses informasi untuk koneksi tersebut di Wilayah tersebut.

Ganti nama koneksi - Ringkasan perubahan

Fitur koneksi di konsol Alat Pengembang memungkinkan Anda menghubungkan AWS sumber daya Anda ke repositori sumber pihak ketiga. Pada 29 Maret 2024, AWS CodeStar Connections diubah namanya menjadi. AWS CodeConnections Bagian berikut menjelaskan bagian-bagian berbeda dari fitur yang berubah dengan penggantian nama, dan tindakan apa yang perlu Anda ambil untuk memastikan bahwa sumber daya Anda terus berfungsi dengan baik.

Perhatikan bahwa daftar ini tidak lengkap. Sementara bagian lain dari produk juga berubah, pembaruan ini adalah yang paling relevan.

Note

Tindakan untuk sumber daya yang dibuat di bawah awalan layanan baru `codeconnections` tersedia. Membuat sumber daya di bawah awalan layanan baru akan digunakan `codeconnections` di sumber daya ARN. Tindakan dan sumber daya untuk awalan `codestar-connections` layanan tetap tersedia. Saat menentukan sumber daya dalam kebijakan IAM, awalan layanan harus sesuai dengan sumber daya.

Note

Mulai 1 Juli 2024, konsol membuat koneksi dengan `codeconnections` ARN sumber daya. Sumber daya dengan kedua awalan layanan akan terus ditampilkan di konsol.

Awalan layanan berganti nama

Koneksi APIs menggunakan awalan layanan yang diganti namanya: `codeconnections`

Untuk menggunakan awalan baru dalam perintah CLI, unduh versi 2. AWS CLI Berikut ini adalah contoh perintah dengan awalan diperbarui.

```
aws codeconnections delete-connection --connection-arn arn:aws:codeconnections:us-west-2:account_id:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Tindakan berganti nama di IAM

Tindakan di IAM menggunakan awalan baru, seperti yang ditunjukkan dalam contoh berikut:

```
codeconnections:CreateConnection
codeconnections>DeleteConnection
codeconnections:GetConnection
codeconnections:ListConnections
```

Sumber daya baru ARN

Sumber daya koneksi yang dibuat akan memiliki ARN baru:

```
arn:aws:codeconnections:us-west-2:account-ID:connection/*
```

Kebijakan peran layanan yang terpengaruh

Untuk layanan berikut, kebijakan peran layanan akan menggunakan awalan baru dalam pernyataan kebijakan. Anda juga dapat memperbarui kebijakan peran layanan yang ada untuk menggunakan izin baru, tetapi kebijakan yang dibuat dengan awalan lama akan terus didukung.

- Kebijakan CodePipeline peran layanan yang dikelola pelanggan
- AWSCodeStarServiceRoleKebijakan peran AWS CodeStar layanan

CloudFormation Sumber daya baru

Untuk menggunakan CloudFormation sumber daya untuk koneksi, sumber daya baru akan tersedia. Sumber daya yang ada masih akan didukung.

- [AWS CloudFormation](#) Sumber daya baru bernama `AWS::CodeConnections::Connection`. Lihat [AWS::CodeConnections::Connection](#) di Panduan CloudFormation Pengguna.
- Sumber daya `AWS::CodeStarConnections::Connection` yang ada masih akan didukung. Lihat [AWS::CodeStarConnections::Connection](#) di Panduan CloudFormation Pengguna.

Riwayat dokumen

Tabel berikut menjelaskan dokumentasi untuk rilis dari konsol Alat Developer.

- AWS CodeStar Versi API Pemberitahuan: 2019-10-15
- AWS CodeConnections Versi API: 2023-12-01

Perubahan	Deskripsi	Tanggal
DevOps Penyedia Azure baru untuk koneksi	Support ditambahkan untuk mengonfigurasi koneksi untuk AWS sumber daya untuk berinteraksi dengan DevOps Azure. Untuk informasi selengkapnya, lihat Membuat sambungan ke Azure DevOps .	Agustus 5, 2025
Kunci kondisi baru untuk host VPC IDs	Anda dapat mengelola akses host untuk Server GitHub Perusahaan dan host yang GitLab dikelola sendiri menggunakan kunci VpcId kondisi. Kunci kondisi memungkinkan Anda untuk menerapkan kebijakan yang terkait dengan membuat atau memperbarui host untuk menggunakan ID VPC tertentu. Untuk informasi selengkapnya, lihat referensi izin koneksi .	Maret 13, 2025
Tambahkan dukungan untuk berbagi koneksi antar akun	Anda dapat melihat dan mengelola koneksi sebagai sumber daya AWS Resource Access Manager, dan Anda	Maret 6, 2025

dapat berbagi koneksi di antaranya Akun AWS. Untuk informasi selengkapnya, lihat [Berbagi koneksi dengan Akun AWS](#).

[Pembaruan untuk menambah dan memperbaiki informasi yang menjelaskan cara kerja koneksi dengan akun pengguna atau organisasi](#)

Ihtisar dan informasi pemecahan masalah diperbarui untuk menjelaskan dengan benar bagaimana koneksi bekerja dengan akun pengguna atau organisasi. Lihat [Cara kerja koneksi](#), [Cara kerja koneksi dengan organisasi](#), dan [Koneksi dan penyiapan host untuk penyedia terinstal yang mendukung organisasi](#). AWS CodeConnections

Desember 9, 2024

[Memperbarui ke kebijakan terkelola untuk koneksi service-linked-role](#)

Kebijakan terkelola untuk peran terkait layanan untuk menggunakan sinkronisasi Git dengan repositori Git telah diperbarui untuk sumber daya dengan kedua awalan layanan. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk AWS CodeConnections dan kebijakan yang dikelola](#).

April 26, 2024

[AWS CodeStar Koneksi berganti nama menjadi AWS CodeConnections](#)

Memperkenalkan AWS CodeConnections, yang memungkinkan Anda membuat dan mengelola koneksi antar AWS sumber daya, seperti pipeline di CodePipeline, ke penyedia Git pihak ketiga.

Maret 29, 2024

[Koneksi ke GitLab sekarang didukung di CodeBuild](#)

Support ditambahkan CodeBuild untuk mengonfigurasi koneksi ke GitLab. Untuk informasi selengkapnya, lihat [Integrasi produk dan layanan dengan AWS CodeConnections](#).

Maret 27, 2024

[Support untuk GitLab Self-Managed](#)

Support ditambahkan untuk mengkonfigurasi koneksi dan host untuk AWS sumber daya untuk berinteraksi dengan GitLab self-managed. Untuk informasi selengkapnya, lihat [Alur kerja untuk membuat atau memperbarui host dan membuat sambungan ke kelola GitLab sendiri](#).

28 Desember 2023

[Tautan repositori baru dan konfigurasi sinkronisasi untuk koneksi](#)

Menambahkan informasi tentang mengonfigurasi tautan repositori dan konfigurasi sinkronisasi. Gunakan konfigurasi sinkronisasi untuk menyinkronkan konten dari repositori Git untuk memperbarui sumber daya CloudFormation tumpukan Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan tautan repositori](#) dan [Bekerja dengan konfigurasi sinkronisasi](#).

27 November 2023

[Support untuk koneksi service-linked-role](#)

Support ditambahkan untuk mengonfigurasi koneksi untuk menggunakan sinkronisasi Git dengan repositori Git. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk AWS CodeConnections dan kebijakan](#) yang [dikelola](#).

26 November 2023

[Support untuk GitLab grup](#)

Support ditambahkan untuk mengkonfigurasi koneksi untuk AWS sumber daya untuk berinteraksi dengan GitLab grup. Untuk informasi selengkapnya, lihat [Membuat sambungan](#) dan [membuat sambungan ke GitLab](#).

15 September 2023

Jenis GitLab penyedia baru	Anda sekarang dapat membuat koneksi ke GitLab. Untuk informasi selengkapnya, lihat Membuat sambungan dan membuat sambungan ke GitLab .	10 Agustus 2023
Jenis target baru untuk aturan notifikasi	Sekarang Anda dapat memilih klien AWS Chatbot yang dikonfigurasi untuk saluran Microsoft Teams sebagai target untuk aturan notifikasi. Untuk informasi selengkapnya, lihat Membuat aturan notifikasi dan Bekerja dengan target aturan notifikasi .	17 Mei 2023
Koneksi tersedia di Wilayah Eropa (Milan)	Menambahkan informasi untuk koneksi di Wilayah Eropa (Milan). Untuk informasi selengkapnya, lihat Lalu lintas antar AWS CodeConnections sumber daya di seluruh Wilayah .	17 Mei 2023
Menambahkan pemecahan masalah untuk kesalahan koneksi dengan izin repositori	Saat membuat koneksi ke repositori di GitHub organisasi, Anda harus menjadi pemilik GitHub organisasi. Untuk informasi selengkapnya, lihat Kesalahan koneksi saat menyambung ke GitHub .	Agustus 29, 2022

Menambahkan informasi untuk menandai sumber daya host	Anda sekarang dapat menandai host menggunakan konsol dan CLI. Untuk informasi selengkapnya, lihat Menandai sumber daya di AWS CodeConnections .	19 April 2021
Dukungan titik akhir VPC untuk koneksi	Anda sekarang dapat menggunakan VPC endpoint dengan koneksi. Untuk informasi selengkapnya, lihat AWS CodeConnections dan antarmuka titik akhir VPC ().AWS PrivateLink	24 November 2020
Jenis penyedia Cloud baru GitHub dan GitHub Enterprise	Anda sekarang dapat membuat koneksi ke GitHub dan GitHub Enterprise Cloud. Untuk informasi selengkapnya, lihat Membuat sambungan dan membuat sambungan ke GitHub .	30 September 2020
Menambahkan jenis penyedia GitHub Enterprise Server dan sumber daya host	Informasi tentang sumber daya host untuk koneksi telah ditambahkan ke panduan ini. Anda sekarang dapat membuat koneksi ke GitHub Enterprise Server. Untuk informasi selengkapnya, lihat Buat koneksi dan Bekerja dengan host . Ini adalah rilis umum ketersediaan fitur koneksi di Panduan Pengguna konsol Alat Developer.	29 Juni 2020

[Menambahkan informasi untuk menggunakan dan menandai koneksi](#)

Informasi tentang fitur koneksi di konsol telah ditambahkan ke panduan ini. Anda dapat melihat konsep, langkah-langkah untuk memulai, referensi izin termasuk kebijakan contoh, dan langkah-langkah untuk membuat, melihat, dan menandai koneksi. Untuk informasi selengkapnya, lihat [Apa itu koneksi](#), [Konsep koneksi](#), [Memulai koneksi](#), [Membuat koneksi](#), [Menandai sumber daya AWS CodeConnections](#), [Keamanan](#), [Kuota untuk koneksi](#), [Pemecahan Masalah](#), dan panggilan [AWS CodeConnections API](#) dengan AWS CloudTrail Untuk melihat daftar tindakan penyedia tambahan (tindakan hanya izin), lihat [Tindakan untuk ProviderType](#).

28 Juni 2020

[Jenis target baru untuk aturan notifikasi](#)

Anda sekarang dapat memilih klien AWS Chatbot yang dikonfigurasi untuk saluran Slack sebagai target untuk aturan notifikasi. Untuk informasi selengkapnya, lihat [Membuat aturan notifikasi](#) dan [Bekerja dengan target aturan notifikasi](#).

2 April 2020

[Menambahkan pemberitahuan tentang AWS CodeCommit acara tambahan](#)

Sekarang Anda dapat mengonfigurasi notifikasi untuk peristiwa yang terkait dengan menarik persetujuan permintaan. Untuk informasi selengkapnya, lihat [Acara untuk aturan notifikasi pada repositori](#) dan [Bekerja dengan permintaan tarik masuk](#).
CodeCommit

10 Februari 2020

[Pemberitahuan tersedia di dua AWS wilayah tambahan](#)

Konsol Alat Developer sekarang mendukung notifikasi di Middle East (Bahrain) dan Asia Pacific (Hong Kong). Untuk informasi selengkapnya, lihat [AWS CodeStar Pemberitahuan](#) di Referensi Umum AWS.

5 Februari 2020

[Menambahkan dukungan untuk topik Amazon SNS terenkripsi](#)

Panduan telah ditambahkan untuk menggunakan topik Amazon SNS topik terenkripsi sebagai target notifikasi. Untuk informasi selengkapnya, lihat [Mengonfigurasi topik Amazon SNS untuk notifikasi](#) .

4 Februari 2020

[Pemberitahuan dapat mencakup informasi tag sesi untuk CodeCommit](#)

Pemberitahuan untuk sekarang CodeCommit dapat berisi informasi identitas pengguna, seperti nama tampilan atau alamat email, melalui penggunaan tag sesi. Untuk informasi selengkapnya, lihat [Konsep](#) dan [Menggunakan tag untuk memberikan informasi identitas CodeCommit](#).

19 Desember 2019

[Rilis awal](#)

Ini adalah rilis awal dari Panduan Pengguna konsol Alat Developer.

5 November 2019

AWS Glosarium

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

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