



Panduan Pengguna

AWS Well-Architected Tool



AWS Well-Architected Tool: 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 di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS Well-Architected Tool?	1
Apa itu AWS Well-Architected Framework?	2
AWS Well-Architected Tool glosarium	2
Memulai	4
Memberikan akses ke AWS WA Tool	4
Mengaktifkan integrasi	5
Mengaktifkan AppRegistry	6
Mengaktifkan Trusted Advisor	7
Menentukan beban kerja	15
Mendokumentasikan beban kerja	18
Meninjau beban kerja	19
Melihat pemeriksaan Trusted Advisor	21
Menyimpan tonggak pencapaian	23
Tutorial: Dokumentasikan beban kerja	24
Langkah 1: Tentukan beban kerja	24
Langkah 2: Dokumentasikan status beban kerja	25
Langkah 3: Tinjau rencana perbaikan	28
Langkah 4: Lakukan perbaikan dan ukur kemajuan	30
Peninjauan Kerangka Kerja Well-Architected (WAFR)	32
Fase WAFR	32
Bersiap untuk WAFR	32
Beban kerja dan cakupan	33
Orang dan budaya	34
Dokumentasi dan infrastruktur	37
Mekanisme	38
Hasil bisnis	39
Sumber daya	40
Menjalankan WAFR	40
Sebelum WAFR	40
Kiat peninjauan	41
Menjalankan WAFR	42
Akses IAM	42
Sumber daya	43
Meningkatkan beban kerja Anda	43

Identifikasi dan pahami risiko	44
Tentukan solusi preskriptif	47
Prioritaskan peningkatan	47
Implementasikan dan lacak peningkatan	49
Jadwal setelah WAFR	50
Beban kerja di AWS Well-Architected Tool	52
Masalah Risiko Tinggi (HRI) dan Masalah Risiko Menengah (MRI)	53
Menentukan beban kerja	54
Melihat beban kerja	55
Mengedit beban kerja	55
Berbagi beban kerja	56
Pertimbangan berbagi	58
Menghapus akses bersama	59
Mengubah akses bersama	60
Menerima dan menolak undangan	61
Menghapus beban kerja	62
Menghasilkan laporan beban kerja	62
Melihat detail beban kerja	63
Tab Ikhtisar	63
Tab Titik Pencapaian	64
Tab Properti	64
Tab Berbagi	64
Lensa	66
Menambahkan lensa	66
Menghapus lensa	67
Melihat detail lensa	67
Tab Gambaran umum	68
Tab Rencana perbaikan	68
Tab Berbagi	68
Lensa kustom	68
Melihat lensa kustom	69
Membuat lensa kustom	70
Melihat pratinjau lensa kustom	71
Memublikasikan lensa kustom	72
Memublikasikan pembaruan lensa	72
Membagikan lensa	74

Menambahkan tanda ke lensa	75
Menghapus lensa	76
Spesifikasi format lensa	76
Peningkatan lensa	83
Menentukan lensa mana yang akan ditingkatkan	84
Meningkatkan lensa	85
Katalog Lensa	86
Template ulasan	89
Membuat template ulasan	89
Mengedit template ulasan	90
Berbagi template ulasan	91
Mendefinisikan beban kerja dari template	92
Menghapus template ulasan	93
Profil	94
Membuat profil	94
Mengedit profil	95
Berbagi profil	95
Menambahkan profil ke beban kerja	96
Menghapus profil dari beban kerja	96
Menghapus profil	97
Jira	99
Menyiapkan konektor	100
Mengkonfigurasi konektor	101
Menyinkronkan beban kerja	103
Menghapus pemasangan konektor	104
Tonggak sejarah	106
Menyimpan tonggak	106
Melihat tonggak	106
Menghasilkan laporan tonggak	107
Bagikan undangan	108
Menerima undangan berbagi	109
Menolak undangan berbagi	109
Notifikasi	111
Pemberitahuan lensa	111
Pemberitahuan profil	111
Dasbor	113

Ringkasan	113
Masalah Kerangka Kerja yang Dirancang dengan Baik per Pilar	113
Masalah Kerangka Kerja yang Dirancang dengan Baik per Beban Kerja	114
Masalah Kerangka Kerja Well-Architected oleh item rencana perbaikan	115
Keamanan	117
Perlindungan data	118
Enkripsi saat diam	119
Enkripsi saat bergerak	119
Cara AWS menggunakan data Anda	119
Manajemen identitas dan akses	120
Audiens	120
Mengautentikasi dengan identitas	120
Mengelola akses menggunakan kebijakan	122
Cara kerja AWS Well-Architected Tool dengan IAM	124
Contoh kebijakan berbasis identitas	129
Kebijakan yang dikelola AWS	136
Pemecahan masalah	143
Respons insiden	143
Validasi kepatuhan	143
Ketahanan	144
Keamanan infrastruktur	144
Analisis konfigurasi dan kerentanan	145
Pencegahan "confused deputy" lintas layanan	145
Berbagai sumber daya Anda	147
Aktifkan pembagian sumber daya dalam AWS Organizations	147
Memberikan tag ke sumber daya Anda	150
Dasar-dasar tag	150
Memberikan tag ke sumber daya Anda	151
Pembatasan tag	152
Mengelola tag menggunakan konsol	153
Menambahkan tag ke sumber daya individu pada saat pembuatan	153
Menambahkan dan menghapus tag pada sumber daya individu	153
Mengelola tag menggunakan API	155
Pencatatan log	156
Informasi AWS WA Tool di CloudTrail	156
Memahami entri file log AWS WA Tool	157

EventBridge	160
Contoh peristiwa dari AWS WA Tool	161
Revisi dokumen	165
AWSGlosarium	172

Apa itu AWS Well-Architected Tool?

AWS Well-Architected Tool (AWS WA Tool) adalah layanan di cloud yang menyediakan proses yang konsisten untuk mengukur arsitektur Anda menggunakan praktik AWS terbaik. AWS WA Tool membantu Anda sepanjang siklus hidup produk dengan melakukan hal berikut:

- Membantu mendokumentasikan keputusan yang Anda buat
- Memberikan rekomendasi untuk meningkatkan beban kerja Anda berdasarkan praktik terbaik
- Membimbing Anda dalam membuat beban kerja Anda lebih andal, aman, efisien, dan hemat biaya

Anda dapat menggunakannya AWS WA Tool untuk mendokumentasikan dan mengukur beban kerja Anda menggunakan praktik terbaik dari AWS Well-Architected Framework. Praktik terbaik ini dikembangkan oleh AWS Solutions Architects berdasarkan pengalaman bertahun-tahun mereka membangun solusi di berbagai bisnis. Kerangka kerja ini memberikan pendekatan yang konsisten untuk mengukur arsitektur dan memberikan panduan untuk menerapkan desain yang sesuai dengan kebutuhan Anda dari waktu ke waktu.

Selain praktik AWS terbaik, Anda dapat menggunakan lensa khusus untuk mengukur beban kerja Anda menggunakan praktik terbaik Anda sendiri. Anda dapat menyesuaikan pertanyaan dalam lensa khusus agar spesifik untuk teknologi tertentu atau untuk membantu Anda memenuhi kebutuhan tata kelola dalam organisasi Anda. Lensa khusus memperluas panduan yang diberikan oleh AWS lensa.

Integrasi dengan [AWS Trusted Advisor](#) dan [AWS Service Catalog AppRegistry](#) membantu Anda lebih mudah menemukan informasi yang diperlukan untuk menjawab pertanyaan AWS Well-Architected Tool ulasan.

Layanan ini ditujukan bagi mereka yang terlibat dalam pengembangan produk teknis, seperti chief technology officer (CTOs), arsitek, pengembang, dan anggota tim operasi. AWS pelanggan menggunakannya AWS WA Tool untuk mendokumentasikan arsitektur mereka, menyediakan tata kelola peluncuran produk, dan untuk memahami dan mengelola risiko dalam portofolio teknologi mereka.

Topik

- [Apa itu AWS Well-Architected Framework?](#)
- [AWS Well-Architected Tool glosarium](#)

Apa itu AWS Well-Architected Framework?

[AWS Well-Architected](#) Framework mendokumentasikan serangkaian pertanyaan mendasar yang memungkinkan Anda memahami bagaimana arsitektur tertentu selaras dengan praktik terbaik cloud. Kerangka kerja ini memberikan pendekatan yang konsisten untuk mengevaluasi sistem terhadap kualitas yang diharapkan dari sistem berbasis cloud modern. Berdasarkan keadaan arsitektur Anda, kerangka kerja menyarankan perbaikan yang dapat Anda lakukan untuk mencapai kualitas tersebut dengan lebih baik.

Dengan menggunakan kerangka kerja, Anda mempelajari praktik terbaik arsitektur untuk merancang dan mengoperasikan sistem yang andal, aman, efisien, dan hemat biaya di cloud. Layanan ini menyediakan cara yang bisa Anda lakukan untuk menilai arsitektur Anda secara terus menerus berdasarkan praktik terbaik dan mengidentifikasi area yang perlu diperbaiki. Kerangka kerja ini didasarkan pada enam pilar: keunggulan operasional, keamanan, keandalan, efisiensi kinerja, optimalisasi biaya, dan keberlanjutan.

Saat merancang beban kerja, Anda membuat trade-off antara pilar-pilar ini berdasarkan kebutuhan bisnis Anda. Keputusan bisnis ini membantu mendorong prioritas teknik Anda. Dalam lingkungan pengembangan, Anda dapat mengoptimalkan untuk mengurangi biaya dengan mengorbankan keandalan. Dalam solusi mission-critical, Anda mungkin mengoptimalkan keandalan dan bersedia menerima peningkatan biaya. Dalam solusi e-commerce, Anda dapat memprioritaskan kinerja, karena kepuasan pelanggan dapat mendorong peningkatan pendapatan. Keamanan dan keunggulan operasional umumnya tidak diperdagangkan dengan pilar lainnya.

Untuk informasi lebih lanjut tentang kerangka kerja, kunjungi situs web [AWS Well-Architected](#).

AWS Well-Architected Tool glosarium

Berikut ini mendefinisikan istilah umum yang digunakan dalam AWS WA Tool dan Kerangka AWS Well-Architected.

- Beban kerja mengidentifikasi serangkaian komponen yang memberikan nilai bisnis. Beban kerja biasanya merupakan tingkat detail yang dikomunikasikan oleh para pemimpin bisnis dan teknologi. Contoh beban kerja termasuk situs web pemasaran, situs web e-commerce, backend untuk aplikasi seluler, dan platform analitik. Beban kerja bervariasi dalam tingkat kompleksitas arsitekturnya. Mereka bisa sederhana, seperti situs web statis, atau kompleks, seperti arsitektur layanan mikro dengan banyak penyimpanan data dan banyak komponen.

- Tonggak sejarah menandai perubahan utama dalam arsitektur Anda saat berevolusi di seluruh siklus hidup produk — desain, pengujian, siaran langsung, dan produksi.
- Lensa menyediakan cara bagi Anda untuk secara konsisten mengukur arsitektur Anda terhadap praktik terbaik dan mengidentifikasi area untuk perbaikan.

Selain lensa yang disediakan oleh AWS, Anda juga dapat membuat dan menggunakan lensa Anda sendiri, atau menggunakan lensa yang telah dibagikan dengan Anda.

- Masalah risiko tinggi (HRIs) adalah pilihan arsitektur dan operasional yang AWS telah ditemukan dapat mengakibatkan dampak negatif yang signifikan terhadap bisnis. Ini HRIs dapat mempengaruhi operasi organisasi, aset, dan individu.
- Masalah risiko menengah (MRIs) adalah pilihan arsitektur dan operasional yang AWS telah ditemukan dapat berdampak negatif pada bisnis, tetapi pada tingkat yang lebih rendah daripada HRIs.

Untuk informasi tambahan, lihat [Masalah Risiko Tinggi \(HRI\) dan Masalah Risiko Menengah \(MRI\)](#).

Memulai dengan AWS Well-Architected Tool

Untuk mulai menggunakan AWS Well-Architected Tool, pertama-tama Anda memberikan izin yang sesuai kepada pengguna, grup, dan peran Anda, serta mengaktifkan dukungan untuk Layanan AWS yang ingin Anda gunakan dengan AWS WA Tool. Selanjutnya, Anda menentukan dan mendokumentasikan beban kerja. Anda juga dapat menyimpan pencapaian untuk status terkini sebuah beban kerja.

Topik berikut menjelaskan cara mulai menggunakan AWS WA Tool. Untuk tutorial langkah demi langkah yang menunjukkan cara menggunakan AWS Well-Architected Tool, lihat [Tutorial: Mendokumentasikan beban kerja AWS Well-Architected Tool](#).

Topik

- [Memberikan akses ke AWS WA Tool untuk pengguna, grup, atau peran](#)
- [Mengaktifkan dukungan di AWS WA Tool untuk layanan AWS lain](#)
- [Menentukan beban kerja di AWS WA Tool](#)
- [Mendokumentasikan beban kerja di AWS WA Tool](#)
- [Meninjau beban kerja dengan Kerangka Kerja AWS Well-Architected](#)
- [Melihat pemeriksaan Trusted Advisor untuk beban kerja Anda](#)
- [Menyimpan tonggak pencapaian untuk beban kerja di AWS WA Tool](#)

Memberikan akses ke AWS WA Tool untuk pengguna, grup, atau peran

Anda dapat memberikan kontrol penuh atau akses hanya baca ke AWS Well-Architected Tool untuk pengguna, grup, atau peran.

Berikan akses ke AWS WA Tool

1. Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:
 - Pengguna dan grup di AWS IAM Identity Center:

Buat rangkaian izin. Ikuti instruksi di [Buat rangkaian izin](#) dalam Panduan Pengguna AWS IAM Identity Center.

- Pengguna yang dikelola di IAM melalui penyedia identitas:

Buat peran untuk federasi identitas. Ikuti instruksi dalam [Buat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) dalam Panduan Pengguna IAM.

- Pengguna IAM:

- Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam [Buat peran untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

- (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam [Menambahkan izin ke pengguna \(konsol\)](#) dalam Panduan Pengguna IAM.

2. Untuk memberikan kontrol penuh, terapkan kebijakan terkelola `WellArchitectedConsoleFullAccess` ke set izin atau peran.

Akses penuh memungkinkan principal melakukan semua tindakan di AWS WA Tool. Akses ini diperlukan untuk menentukan beban kerja, menghapus beban kerja, melihat beban kerja, memperbarui beban kerja, membagikan beban kerja, membuat lensa kustom, dan membagikan lensa kustom.

3. Untuk memberikan akses hanya baca, terapkan kebijakan terkelola `WellArchitectedConsoleReadOnlyAccess` ke set izin atau peran. Principal dengan peran ini hanya dapat melihat sumber daya.

Untuk informasi selengkapnya tentang kebijakan-kebijakan ini, lihat [Kebijakan yang dikelola AWS untuk AWS Well-Architected Tool](#).

Mengaktifkan dukungan di AWS WA Tool untuk layanan AWS lain

Mengaktifkan akses Organisasi akan memungkinkan AWS Well-Architected Tool mengumpulkan informasi tentang struktur organisasi Anda agar dapat berbagi sumber daya dengan lebih mudah (lihat [the section called “Aktifkan pembagian sumber daya dalam AWS Organizations”](#) untuk informasi selengkapnya). Mengaktifkan dukungan Penemuan akan mengumpulkan informasi dari [AWS Trusted Advisor](#), [AWS Service Catalog AppRegistry](#), dan sumber daya terkait (seperti tumpukan CloudFormation dalam kumpulan sumber daya AppRegistry) untuk mempermudah Anda menemukan informasi yang diperlukan dalam menjawab pertanyaan peninjauan Well-Architected, dan menyesuaikan pemeriksaan Trusted Advisor untuk beban kerja.

Mengaktifkan dukungan untuk AWS Organizations, atau mengaktifkan dukungan Penemuan akan secara otomatis membuat peran terkait layanan untuk akun Anda.

Guna mengaktifkan dukungan untuk layanan lain yang dapat menerima interaksi AWS WA Tool, buka Pengaturan.

1. Untuk mengumpulkan informasi dari AWS Organizations, aktifkan opsi Aktifkan dukungan AWS Organizations.
2. Aktifkan opsi Aktifkan dukungan Penemuan untuk mengumpulkan informasi dari layanan dan sumber daya AWS lain.
3. Pilih Lihat izin peran untuk melihat izin peran terkait layanan atau kebijakan hubungan kepercayaan.
4. Pilih Simpan pengaturan.

Mengaktifkan AppRegistry untuk beban kerja

Menggunakan AppRegistry bersifat opsional, dan pelanggan AWS Business Support dan Enterprise Support dapat mengaktifkannya per beban kerja.

Setiap kali dukungan Penemuan diaktifkan dan AppRegistry dikaitkan dengan beban kerja baru atau yang sudah ada, AWS Well-Architected Tool akan membuat grup atribut yang dikelola layanan. Grup atribut Metadata di AppRegistry berisi ARN beban kerja, nama beban kerja, dan risiko yang terkait dengan beban kerja.

- Ketika dukungan Penemuan diaktifkan, setiap kali ada perubahan pada beban kerja, grup atribut akan diperbarui.
- Ketika dukungan Penemuan dinonaktifkan atau aplikasi dihapus dari beban kerja, informasi beban kerja dihapus dari AWS Service Catalog.

Jika Anda ingin aplikasi AppRegistry mendorong data yang diambil dari Trusted Advisor, tetapkan Definisi sumber daya untuk beban kerja Anda sebagai AppRegistry atau Semua. Buat peran untuk semua akun yang merupakan pemilik atas sumber daya dalam aplikasi Anda dengan mengikuti pedoman di [the section called “Mengaktifkan Trusted Advisor di IAM”](#).

Mengaktifkan AWS Trusted Advisor untuk beban kerja

Anda dapat secara opsional mengintegrasikan AWS Trusted Advisor dan mengaktifkannya per beban kerja untuk pelanggan AWS Business Support dan Enterprise Support. Tidak ada biaya untuk mengintegrasikan Trusted Advisor dengan AWS WA Tool, tetapi untuk detail harga Trusted Advisor, lihat [Paket Dukungan AWS](#). Mengaktifkan Trusted Advisor beban kerja dapat memberi Anda pendekatan yang lebih komprehensif, otomatis, dan terpantau untuk meninjau dan mengoptimalkan beban kerja AWS Anda. Hal ini dapat membantu Anda meningkatkan keandalan, keamanan, performa, dan optimalisasi biaya untuk beban kerja Anda.

Guna mengaktifkan Trusted Advisor untuk beban kerja

1. Guna mengaktifkan Trusted Advisor, pemilik beban kerja dapat menggunakan AWS WA Tool untuk memperbarui beban kerja yang ada, atau membuat beban kerja baru dengan memilih Tentukan beban kerja.
2. Masukkan ID akun yang digunakan oleh Trusted Advisor di bidang ID akun, pilih ARN aplikasi di bidang Aplikasi, atau keduanya untuk mengaktifkan Trusted Advisor.
3. Di bagian AWS Trusted Advisor, pilih Aktifkan Trusted Advisor.

Account IDs - optional
Type the IDs of the AWS accounts your workload spans across

111122223333

Specify up to 100 unique account IDs separated by commas

Application - optional [Info](#)
An application is a custom collection of resources, metadata, and tags that performs a function to deliver business value. Your application's Amazon Resource Name (ARN) is a unique identifier for an AWS resource, which is maintained by AppRegistry.

arn:aws:servicecatalog:us-west-2:111122223333/application/#####

Architectural design - optional
A link to your architectural design

The URL can be up to 2048 characters and must begin with one of the follow protocols: [http, https, ftp]. 2048 characters remaining

Industry type - optional
The industry that your workload is associated with

Choose an industry type

Industry - optional
The category within your industry that your workload is associated with

Choose a industry


AWS Trusted Advisor - new


AWS Trusted Advisor [Info](#)
Trusted Advisor uses information from your AWS Regions and account IDs entered above to aid workload reviews, providing you automated context for supported questions.

Activate Trusted Advisor

Resource definition
Choose how resources are selected for Trusted Advisor checks.


AppRegistry

 **Additional setup needed**
To pull Trusted Advisor data from other accounts, grant permissions to the AWS Well-Architected Tool to access Trusted Advisor data.

View AWS documentation 

Trusted Advisor checks ✕

AWS Trusted Advisor provides recommendations that help you follow AWS best practices. Trusted Advisor evaluates your account by using checks. These checks identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas. You can then follow the recommendations to optimize your services and resources. Activating Trusted Advisor support aids workload reviews by providing automated context for supported questions.

[Trusted Advisor documentation](#) 

4. Notifikasi bahwa Peran layanan IAM akan dibuat akan ditampilkan saat Trusted Advisor pertama kali diaktifkan untuk beban kerja. Memilih opsi Lihat izin akan menampilkan izin peran IAM. Anda dapat melihat Nama peran, serta Izin dan Hubungan kepercayaan yang dibuat JSON secara otomatis untuk Anda di IAM. Setelah peran dibuat, untuk beban kerja berikutnya yang mengaktifkan Trusted Advisor, hanya notifikasi Pengaturan tambahan diperlukan yang akan ditampilkan.
5. Di menu dropdown Definisi sumber daya, Anda dapat memilih Metadata Beban Kerja, AppRegistry, atau Semua. Memilih opsi Definisi sumber daya akan menentukan data mana yang diambil AWS WA Tool dari Trusted Advisor untuk memberikan pemeriksaan status dalam peninjauan beban kerja yang dipetakan menurut praktik terbaik Well-Architected.

Metadata Beban Kerja – beban kerja ditentukan menurut ID akun dan Region AWS yang ditentukan dalam beban kerja.

AppRegistry – beban kerja ditentukan menurut sumber daya (seperti tumpukan CloudFormation) yang ada dalam aplikasi AppRegistry yang terkait dengan beban kerja.

Semua – beban kerja ditentukan menurut metadata beban kerja dan sumber daya AppRegistry.

6. Pilih Berikutnya.
7. Terapkan Kerangka Kerja AWS Well-Architected ke beban kerja Anda, dan pilih Tentukan beban kerja. Pemeriksaan Trusted Advisor hanya terkait dengan Kerangka Kerja AWS Well-Architected, dan bukan lensa lainnya.

AWS WA Tool secara berkala mendapatkan data dari Trusted Advisor menggunakan peran yang dibuat di IAM. Peran IAM secara otomatis dibuat untuk pemilik beban kerja. Namun, untuk melihat informasi Trusted Advisor, pemilik akun terkait pada beban kerja harus membuka IAM dan membuat peran. Lihat [???](#) untuk detail selengkapnya. Jika peran ini tidak ada, AWS WA Tool tidak dapat memperoleh informasi Trusted Advisor untuk akun tersebut dan akan menampilkan kesalahan.

Untuk informasi selengkapnya tentang membuat peran di AWS Identity and Access Management (IAM), lihat [Membuat peran untuk layanan AWS \(konsol\)](#) dalam Panduan Pengguna IAM.

Mengaktifkan Trusted Advisor untuk beban kerja di IAM

Note

Pemilik beban kerja harus memilih opsi Aktifkan dukungan Penemuan untuk akun mereka sebelum membuat beban kerja Trusted Advisor. Memilih opsi Aktifkan dukungan Penemuan akan membuat peran yang diperlukan untuk pemilik beban kerja. Gunakan langkah-langkah berikut untuk semua akun terkait lainnya.

Pemilik akun terkait untuk beban kerja yang telah mengaktifkan Trusted Advisor harus membuat peran dalam IAM untuk melihat informasi Trusted Advisor di AWS Well-Architected Tool.

Untuk membuat peran dalam IAM AWS WA Tool guna mendapatkan informasi dari Trusted Advisor

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

2. Di panel navigasi konsol IAM, pilih Peran, lalu pilih Buat peran.
3. Di bagian Jenis entitas tepercaya, pilih Kebijakan kepercayaan kustom.
4. Salin dan tempelkan Kebijakan kepercayaan kustom berikut ke bidang JSON di konsol IAM, seperti yang ditunjukkan pada gambar berikut. Ganti **WORKLOAD_OWNER_ACCOUNT_ID** dengan ID akun pemilik beban kerja, dan pilih Berikutnya.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "wellarchitected.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
        },
        "ArnEquals": {
          "aws:SourceArn":
            "arn:aws:wellarchitected:*:111122223333:workload/*"
        }
      }
    }
  ]
}
```

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Service": "wellarchitected.amazonaws.com"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {
11        "StringEquals": {
12          "aws:SourceAccount": "111122223333"
13        },
14        "ArnEquals": {
15          "aws:SourceArn": "arn:aws:wellarchitected:*:111122223333:workload/*"
16        }
17      }
18    }
19  ]
20 }

```

Edit statement Remove

1. Add actions for STS

Q

All actions (sts:)

Access level - read or write

AssumeRole ⓘ

AssumeRoleWithSAML ⓘ

AssumeRoleWithWebIdentity ⓘ

DecodeAuthorizationMessage ⓘ

GetAccessKeyInfo ⓘ

GetCallerIdentity ⓘ

GetFederationToken ⓘ

GetServiceBearerToken ⓘ

GetSessionToken ⓘ

SetSourceIdentity ⓘ

2. Add a principal Add

3. Add a condition (optional) Add

+ Add new statement

JSON Ln 12, Col 3

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0 Preview external access

CancelNext**Note**

aws:sourceArn di blok kondisi dalam kebijakan kepercayaan kustom sebelumnya adalah "arn:aws:wellarchitected:*:**WORKLOAD_OWNER_ACCOUNT_ID**:workload/*", yang merupakan kondisi umum yang menyatakan peran ini dapat digunakan AWS WA Tool untuk semua beban kerja dari pemilik beban kerja. Namun, akses dapat dipersempit ke ARN beban kerja tertentu, atau set ARN beban kerja. Untuk menentukan beberapa ARN, lihat contoh kebijakan kepercayaan berikut.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "wellarchitected.amazonaws.com"
      },

```

```

    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:wellarchitected:us-east-1:111122223333:workload/WORKLOAD_ID_1",
          "arn:aws:wellarchitected:us-east-1:111122223333:workload/WORKLOAD_ID_2"
        ]
      }
    }
  }
]
}

```

5. Pada halaman Tambahkan izin, untuk Kebijakan Izin, pilih Buat kebijakan untuk memberi AWS WA Tool akses untuk membaca data dari Trusted Advisor. Memilih opsi Buat kebijakan akan membuka jendela baru.

Note

Selain itu, Anda memiliki opsi untuk melewati pembuatan izin selama pembuatan peran dan membuat kebijakan inline setelah membuat peran. Pilih Lihat peran dalam pesan pembuatan peran berhasil dan pilih Buat kebijakan inline dari menu dropdown Tambahkan izin di tab Izin.

6. Salin dan tempelkan Kebijakan izin berikut ke dalam bidang JSON. Di Resource ARN, ganti **YOUR_ACCOUNT_ID** dengan ID akun Anda sendiri, tentukan Wilayah atau tanda bintang (*), dan pilih Berikutnya: Tanda.

Untuk detail tentang format ARN, lihat [Amazon Resource Name \(ARN\)](#) dalam Panduan Referensi Umum AWS.

JSON

```

{
  "Version": "2012-10-17",

```

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "trustedadvisor:DescribeCheckRefreshStatuses",
      "trustedadvisor:DescribeCheckSummaries",
      "trustedadvisor:DescribeRiskResources",
      "trustedadvisor:DescribeAccount",
      "trustedadvisor:DescribeRisk",
      "trustedadvisor:DescribeAccountAccess",
      "trustedadvisor:DescribeRisks",
      "trustedadvisor:DescribeCheckItems"
    ],
    "Resource": [
      "arn:aws:trustedadvisor:*:111122223333:checks/*"
    ]
  }
]
}

```

7. Jika Trusted Advisor diaktifkan untuk beban kerja dan Definisi sumber daya ditetapkan ke AppRegistry atau Semua, semua akun yang memiliki sumber daya dalam aplikasi AppRegistry yang dilampirkan ke beban kerja tersebut harus menambahkan izin berikut ke Kebijakan izin untuk peran Trusted Advisor-nya.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DiscoveryPermissions",
      "Effect": "Allow",
      "Action": [
        "servicecatalog:ListAssociatedResources",
        "tag:GetResources",
        "servicecatalog:GetApplication",
        "resource-groups:ListGroupResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource": "*"
    }
  ]
}

```

```
}  
  ]  
}
```

8. (Opsional) Tambahkan tanda. Pilih Berikutnya: Tinjauan.
9. Tinjau kebijakan, beri nama, dan pilih Buat kebijakan.
10. Pada halaman Tambahkan izin untuk peran tersebut, pilih nama kebijakan yang baru saja Anda buat, lalu pilih Berikutnya.
11. Masukkan Nama peran, yang harus menggunakan sintaks berikut:
`WellArchitectedRoleForTrustedAdvisor-WORKLOAD_OWNER_ACCOUNT_ID` dan pilih Buat peran. Ganti *WORKLOAD_OWNER_ACCOUNT_ID* dengan ID akun pemilik beban kerja.

Anda akan mendapatkan pesan berhasil di bagian atas halaman yang memberi tahu Anda bahwa peran telah dibuat.
12. Untuk melihat peran dan kebijakan izin terkait, di panel navigasi kiri pada bagian Manajemen akses, pilih Peran dan cari nama `WellArchitectedRoleForTrustedAdvisor-WORKLOAD_OWNER_ACCOUNT_ID`. Pilih nama peran untuk memverifikasi bahwa Izin dan Hubungan kepercayaan sudah benar.

Menonaktifkan Trusted Advisor untuk beban kerja

Guna menonaktifkan Trusted Advisor untuk beban kerja

Anda dapat menonaktifkan Trusted Advisor untuk beban kerja apa pun dari AWS Well-Architected Tool dengan mengedit beban kerja Anda dan membatalkan pilihan Aktifkan Trusted Advisor. Untuk informasi selengkapnya tentang cara mengedit beban kerja, lihat [the section called “Mengedit beban kerja”](#).

Menonaktifkan Trusted Advisor dari AWS WA Tool tidak akan menghapus peran yang dibuat di IAM. Menghapus peran dari IAM memerlukan tindakan pembersihan terpisah. Pemilik beban kerja atau pemilik akun terkait harus menghapus peran IAM yang dibuat saat Trusted Advisor dinonaktifkan di AWS WA Tool, atau menghentikan AWS WA Tool mengumpulkan data Trusted Advisor untuk beban kerja.

Untuk menghapus **WellArchitectedRoleForTrustedAdvisor** di IAM

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

2. Di panel navigasi konsol IAM, pilih Peran.
3. Cari `WellArchitectedRoleForTrustedAdvisor-WORKLOAD_OWNER_ACCOUNT_ID` dan pilih nama peran.
4. Pilih Hapus. Di jendela pop-up, ketikkan nama peran untuk mengonfirmasi penghapusan, dan pilih Hapus lagi.

Untuk informasi selengkapnya tentang menghapus peran dari IAM, lihat [Menghapus peran IAM \(konsol\)](#) dalam Panduan Pengguna IAM.

Menentukan beban kerja di AWS WA Tool

Beban kerja adalah serangkaian komponen yang memberikan nilai bisnis. Misalnya, beban kerja dapat berupa situs web pemasaran, situs web e-commerce, backend untuk aplikasi seluler, dan platform analitik. Menentukan beban kerja secara akurat akan membantu memastikan peninjauan komprehensif berdasarkan pilar Kerangka Kerja AWS Well-Architected.

Untuk menentukan beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Jika Anda pertama kali menggunakan AWS WA Tool, Anda akan melihat halaman yang memperkenalkan Anda dengan fitur layanan. Di bagian Tentukan beban kerja, pilih Tentukan beban kerja.

Atau, di panel navigasi kiri, pilih Beban kerja dan pilih Tentukan beban kerja.

Untuk detail tentang cara AWS menggunakan data beban kerja Anda, pilih Mengapa AWS memerlukan data ini, dan bagaimana data tersebut akan digunakan?

3. Di kotak Nama, masukkan nama untuk beban kerja Anda.

Note

Nama harus berisi antara 3 dan 100 karakter. Setidaknya tiga karakter tidak boleh berupa spasi. Nama beban kerja harus unik. Spasi dan kapitalisasi akan diabaikan saat memeriksa keunikan.

4. Di kotak Deskripsi, masukkan deskripsi. Nama harus berisi antara 3 dan 250 karakter.

5. Di kotak Pemilik tinjauan, masukkan nama, alamat email, atau pengidentifikasi untuk grup atau individu utama yang merupakan pemilik proses peninjauan beban kerja.
6. Di kotak Lingkungan, pilih lingkungan untuk beban kerja Anda:
 - Produksi – Beban kerja berjalan di lingkungan produksi.
 - Pra-produksi - Beban kerja berjalan di lingkungan pra-produksi.
7. Di bagian Wilayah, pilih Wilayah untuk beban kerja Anda:
 - Region AWS – Pilih Region AWS tempat beban kerja Anda berjalan, satu per satu.
 - Wilayah non-AWS – Masukkan nama Wilayah di luar AWS tempat beban kerja Anda berjalan. Anda dapat menentukan hingga lima Wilayah unik, yang dipisahkan dengan koma.

Gunakan kedua opsi tersebut jika sesuai untuk beban kerja Anda.

8. (Opsional) Di kotak ID akun, masukkan ID Akun AWS yang terkait dengan beban kerja Anda. Anda dapat menentukan hingga 100 ID akun unik, yang dipisahkan dengan koma.

Jika Trusted Advisor diaktifkan, ID akun apa pun yang ditentukan akan digunakan untuk mendapatkan data dari Trusted Advisor. Lihat [Mengaktifkan beban kerja AWS Trusted Advisor untuk beban kerja](#) guna memberikan izin AWS WA Tool untuk mendapatkan data Trusted Advisor atas nama Anda dalam IAM.

9. (Opsional) Di kotak Aplikasi, masukkan ARN aplikasi untuk aplikasi dari [AWS Service Catalog AppRegistry](#) yang ingin Anda kaitkan dengan beban kerja ini. Hanya satu ARN yang dapat ditentukan per beban kerja, dan aplikasi serta beban kerja harus berada di Wilayah yang sama.
10. (Opsional) Di kotak Rancangan arsitektur, masukkan URL untuk rancangan arsitektur Anda.
11. (Opsional) Di kotak Jenis industri, pilih jenis industri yang terkait dengan beban kerja Anda.
12. (Opsional) Di kotak Industri, pilih industri yang paling sesuai dengan beban kerja Anda.
13. (Opsional) Di bagian Trusted Advisor, guna mengaktifkan pemeriksaan Trusted Advisor untuk beban kerja Anda, pilih Aktifkan Trusted Advisor. Pengaturan tambahan mungkin diperlukan untuk akun yang terkait dengan beban kerja Anda. Lihat [the section called “Mengaktifkan Trusted Advisor”](#) guna memberi AWS WA Tool izin untuk mendapatkan data Trusted Advisor atas nama Anda. Pilih dari Metadata Beban Kerja, AppRegistry, atau Semua di bagian Definisi sumber daya untuk menentukan sumber daya apa yang digunakan AWS WA Tool untuk menjalankan pemeriksaan Trusted Advisor.
14. (Opsional) Di bagian Jira, guna mengaktifkan pengaturan sinkronisasi Jira tingkat beban kerja untuk beban kerja, pilih Timpa pengaturan tingkat akun. Pengaturan tambahan mungkin diperlukan untuk akun yang terkait dengan beban kerja Anda. Lihat [Konektor AWS Well-Architected Tool untuk Jira](#) guna memulai pengaturan dan konfigurasi konektor. Pilih dari

Jangan sinkronkan beban kerja, Sinkronkan beban kerja - Manual, dan Sinkronkan beban kerja - Otomatis, dan secara opsional masukkan Kunci proyek Jira yang akan disinkronkan.

Note

Jika Anda tidak menimpa pengaturan tingkat akun, beban kerja akan secara default ditetapkan ke pengaturan sinkronisasi Jira tingkat akun.

15. (Opsional) Di bagian Tanda, tambahkan tanda yang ingin Anda kaitkan dengan beban kerja.

Untuk informasi selengkapnya tentang tanda, lihat [Memberikan tag ke sumber daya AWS WA Tool Anda](#).

16. Pilih Berikutnya.

Jika kotak yang wajib diisi kosong atau jika nilai yang ditentukan tidak valid, Anda harus memperbaiki masalahnya sebelum dapat melanjutkan.

17. (Opsional) Pada langkah Terapkan Profil, kaitkan profil ke beban kerja dengan memilih profil yang ada, mencari nama profil, atau memilih Buat profil untuk [membuat profil](#). Pilih Berikutnya.

18. Pilih lensa yang berlaku untuk beban kerja ini. Hingga 20 lensa dapat ditambahkan ke beban kerja. Untuk deskripsi lensa AWS resmi, lihat [Lensa](#).

Lensa dapat dipilih dari [Lensa kustom](#) (lensa yang Anda buat atau yang dibagikan ke Akun AWS Anda), [Katalog Lensa](#) (lensa AWS resmi yang tersedia untuk semua pengguna), atau keduanya.

Note

Bagian Lensa kustom kosong jika Anda belum membuat lensa kustom atau memiliki lensa kustom yang dibagikan kepada Anda.

Penafian

Dengan mengakses dan/atau menerapkan lensa kustom yang dibuat oleh pengguna atau akun AWS lain, Anda menyatakan bahwa lensa kustom yang dibuat oleh pengguna lain dan dibagikan kepada Anda adalah Konten Pihak Ketiga sebagaimana didefinisikan dalam Perjanjian Pelanggan AWS.

19. Pilih Tentukan beban kerja.

Jika kotak yang wajib diisi kosong atau jika nilai yang ditentukan tidak valid, Anda harus memperbaiki masalahnya sebelum beban kerja Anda ditentukan.

Mendokumentasikan beban kerja di AWS WA Tool

Setelah menentukan beban kerja di AWS Well-Architected Tool, Anda dapat mendokumentasikan statusnya dengan membuka halaman Tinjau beban kerja. Hal ini membantu Anda menilai beban kerja Anda dan melacak progresnya dari waktu ke waktu.

Untuk mendokumentasikan status beban kerja

1. Setelah Anda awalnya menentukan beban kerja, Anda melihat halaman yang menunjukkan detail terkini beban kerja Anda. Pilih Mulai meninjau untuk memulai.

Atau, di panel navigasi kiri, pilih Beban kerja dan pilih nama beban kerja untuk membuka halaman detail beban kerja. Pilih Lanjutkan peninjauan.

(Opsional) Jika profil dikaitkan dengan beban kerja Anda, maka panel navigasi kiri akan berisi daftar pertanyaan peninjauan beban kerja yang Diprioritaskan yang dapat Anda gunakan untuk mempercepat proses peninjauan beban kerja.

2. Anda sekarang akan diberi pertanyaan pertama. Untuk setiap pertanyaan:
 - a. Baca pertanyaan dan tentukan apakah pertanyaan ini berlaku untuk beban kerja Anda.

Untuk panduan tambahan, pilih Info dan lihat informasinya di panel bantuan.

- Jika pertanyaan tidak berlaku untuk beban kerja Anda, pilih Pertanyaan tidak berlaku untuk beban kerja ini.
- Atau, pilih praktik terbaik yang saat ini Anda ikuti dari daftar.

Jika saat ini Anda tidak mengikuti salah satu praktik terbaik, pilih Tidak satu pun.

Untuk panduan tambahan tentang item apa pun, pilih Info dan lihat informasinya di panel bantuan.

- b. (Opsional) Jika satu atau beberapa praktik terbaik tidak berlaku untuk beban kerja Anda, pilih Tandai praktik terbaik yang tidak berlaku untuk beban kerja ini. Untuk setiap praktik terbaik yang dipilih, Anda dapat secara opsional memilih alasan dan memberikan detail tambahan.

- c. (Opsional) Gunakan kotak Catatan untuk merekam informasi yang terkait dengan pertanyaan.

Misalnya, Anda dapat menjelaskan mengapa pertanyaan tidak berlaku atau memberikan detail tambahan tentang praktik terbaik yang dipilih.

- d. Pilih Berikutnya untuk melanjutkan ke pertanyaan berikutnya.

Ulangi langkah-langkah ini untuk setiap pertanyaan di tiap pilar.

3. Pilih Simpan dan keluar kapan saja untuk menyimpan perubahan dan menjeda proses pendokumentasian beban kerja Anda.

Setelah Anda mendokumentasikan beban kerja Anda, Anda dapat kembali ke pertanyaan untuk lanjut meninjaunya kapan saja. Untuk informasi selengkapnya, lihat [Meninjau beban kerja dengan Kerangka Kerja AWS Well-Architected](#).

Meninjau beban kerja dengan Kerangka Kerja AWS Well-Architected

Anda dapat meninjau beban kerja Anda di konsol pada halaman Tinjau beban kerja. Halaman ini menyediakan praktik terbaik dan sumber daya yang bermanfaat untuk performa beban kerja Anda.

The screenshot shows the AWS Well-Architected Tool interface. On the left, a navigation panel lists various questions categorized by pillar (REL, SEC, COST, PERF). The main content area displays a question titled 'PERF 1. How do you evolve your workload to take advantage of new releases?' with options to 'Ask an expert', 'Question does not apply to this workload', and 'Select from the following'. The 'Select from the following' section includes options like 'Stay up-to-date on new resources and services', 'Evolve workload performance over time', and 'Define a process to improve workload performance'. A right-hand panel titled 'Helpful resources' provides links to AWS Blog, YouTube channels, and other resources. Red circles 1, 2, and 3 highlight the navigation panel, the main question, and the helpful resources panel, respectively.

1. Untuk membuka halaman Tinjau beban kerja, dari halaman detail beban kerja, pilih Lanjutkan peninjauan. Panel navigasi kiri menunjukkan pertanyaan untuk setiap pilar. Pertanyaan yang telah Anda jawab ditandai Selesai. Jumlah pertanyaan yang dijawab di setiap pilar ditampilkan di sebelah nama pilar.

Anda dapat menavigasi ke pertanyaan di pilar lain dengan memilih nama pilar lalu memilih pertanyaan yang ingin Anda jawab.

(Opsional) Jika profil dikaitkan dengan beban kerja Anda, maka AWS WA Tool akan menggunakan informasi di profil ini untuk menentukan pertanyaan mana dalam peninjauan beban kerja yang diprioritaskan dan pertanyaan mana yang tidak berlaku untuk bisnis Anda. Di panel navigasi kiri, Anda dapat menggunakan pertanyaan yang Diprioritaskan untuk membantu mempercepat proses peninjauan beban kerja. Ikon notifikasi muncul di samping pertanyaan yang baru ditambahkan ke daftar pertanyaan yang Diprioritaskan.

2. Panel tengah menampilkan pertanyaan saat ini. Pilih praktik terbaik yang Anda ikuti. Pilih Info untuk mendapatkan informasi tambahan tentang pertanyaan atau praktik terbaik. Pilih Tanyakan

pada ahli untuk mengakses komunitas AWS re:Post khusus untuk [AWS Well-Architected](#). AWS re:Post adalah pengganti komunitas tanya jawab berbasis topik untuk Forum AWS. Dengan re:Post, Anda dapat menemukan jawaban, menjawab pertanyaan, bergabung dengan grup, mengikuti topik populer, serta memberikan suara pada pertanyaan dan jawaban favorit Anda.

(Opsional) Untuk menandai satu atau beberapa praktik terbaik sebagai tidak berlaku, pilih Tandai praktik terbaik yang tidak berlaku untuk beban kerja ini dan pilih praktik terbaiknya.

Gunakan tombol di bagian bawah panel ini untuk membuka pertanyaan berikutnya, kembali ke pertanyaan sebelumnya, atau menyimpan perubahan Anda dan keluar.

- Panel bantuan yang tepat menampilkan informasi tambahan dan sumber daya yang bermanfaat. Pilih Tanyakan pada ahli untuk mengakses komunitas AWS re:Post khusus untuk [AWS Well-Architected](#). Di komunitas ini, Anda dapat mengajukan pertanyaan terkait dengan merancang, membangun, melakukan deployment, dan mengoperasikan beban kerja di AWS.

Melihat pemeriksaan Trusted Advisor untuk beban kerja Anda

Jika Trusted Advisor diaktifkan untuk beban kerja Anda, tab Pemeriksaan Trusted Advisor ditampilkan di sebelah Pertanyaan. Jika ada pemeriksaan yang tersedia untuk praktik terbaik, notifikasi bahwa ada pemeriksaan Trusted Advisor yang tersedia akan ditampilkan setelah pemilihan pertanyaan. Memilih Lihat pemeriksaan akan membawa Anda ke tab Pemeriksaan Trusted Advisor.

The screenshot displays the AWS Well-Architected Tool interface. On the left, a sidebar lists various cost-related questions (COST 3 to COST 10). The main content area is titled 'Question' and 'Trusted Advisor checks'. It features a question: 'COST 5. How do you evaluate cost when you select services?'. Below the question, there is a list of options to select from, such as 'Identify organization requirements for cost', 'Analyze all components of this workload', etc. A red box highlights a notification at the bottom of the main content area that reads: 'Trusted Advisor checks available. To help you answer the question, we have automated checks that will give you more context on what you have in your account.' A 'View checks' button is also visible next to the notification. On the right, there is a 'Helpful resources' panel with links to 'Cloud products', 'Amazon S3 storage classes', and 'AWS Total Cost of Ownership (TCO) Calculator'.

Pada tab Pemeriksaan Trusted Advisor, Anda dapat melihat informasi yang lebih mendetail tentang pemeriksaan praktik terbaik dari Trusted Advisor, melihat tautan ke dokumentasi Trusted Advisor

di panel Sumber daya bantuan, atau Unduh detail pemeriksaan, yang menyediakan laporan pemeriksaan Trusted Advisor dan status untuk setiap praktik terbaik dalam file CSV.

The screenshot shows the AWS Well-Architected Framework interface. On the left, there is a sidebar with navigation links for various cost-related checks (COST 5-10) and a 'Sustainability' section with a '0/6' indicator. The main content area is titled 'AWS Well-Architected Framework' and shows a list of 'Trusted Advisor checks'. The checks listed are:

- Savings Plan** (Info): Account statuses 2 (Green)
- Amazon ElastiCache Reserved Node Optimization** (Info): Account statuses 2 (Green)
- Amazon EC2 Reserved Instances Optimization** (Info): Account statuses 2 (Green)
- Amazon OpenSearch Service Reserved Instance Optimization** (Info): Account statuses 2 (Green)
- Amazon Redshift Reserved Node Optimization** (Info): Account statuses 1 (Yellow), 1 (Green)
- Amazon Relational Database Service (RDS) Reserved Instance Optimization** (Info): Account statuses 2 (Green)

On the right, a detailed view for 'Amazon Redshift Reserved Node Optimization' is shown. It includes an 'Investigation recommended' warning (yellow triangle) and a summary of account statuses: '1 Investigation recommended' (yellow triangle) and '1 No problems detected' (green checkmark).

Kategori pemeriksaan dari Trusted Advisor ditampilkan sebagai ikon berwarna, dan nomor di samping setiap ikon menunjukkan jumlah akun yang berada dalam status tersebut.

- Tindakan yang direkomendasikan (merah) – Trusted Advisor merekomendasikan tindakan untuk pemeriksaan.
- Investigasi yang direkomendasikan (kuning) – Trusted Advisor mendeteksi kemungkinan masalah untuk pemeriksaan.
- Tidak ada masalah yang terdeteksi (hijau) – Trusted Advisor tidak mendeteksi masalah untuk pemeriksaan.
- Item yang dikecualikan (abu-abu) - Jumlah pemeriksaan yang memiliki item yang dikecualikan, seperti sumber daya yang Anda inginkan agar diabaikan oleh pemeriksaan.

Untuk informasi selengkapnya tentang pemeriksaan yang disediakan Trusted Advisor, lihat [Melihat kategori pemeriksaan](#) dalam Panduan Pengguna Dukungan.

Memilih tautan Info di samping setiap pemeriksaan Trusted Advisor akan menampilkan informasi tentang pemeriksaan di panel Sumber daya bantuan. Untuk informasi selengkapnya, lihat [Referensi pemeriksaan AWS Trusted Advisor](#) dalam Panduan Pengguna Dukungan.

Menyimpan tonggak pencapaian untuk beban kerja di AWS WA Tool

Anda dapat menyimpan tonggak pencapaian untuk beban kerja kapan saja. Tonggak pencapaian mencatat status beban kerja saat ini.

Untuk menyimpan tonggak pencapaian

1. Dari halaman detail beban kerja, pilih Simpan tonggak pencapaian.
2. Di kotak Nama tonggak pencapaian, masukkan nama untuk tonggak pencapaian Anda.

Note

Nama harus berisi antara 3 dan 100 karakter. Setidaknya tiga karakter tidak boleh berupa spasi. Nama tonggak pencapaian yang terkait dengan beban kerja harus unik. Spasi dan kapitalisasi akan diabaikan saat memeriksa keunikan.

3. Pilih Simpan.

Setelah tonggak pencapaian disimpan, Anda tidak dapat mengubah data beban kerja yang direkam dalam tonggak pencapaian tersebut.

Lihat informasi yang lebih lengkap di [Tonggak sejarah](#).

Tutorial: Dokumentasikan beban AWS Well-Architected Tool kerja

Tutorial ini menjelaskan penggunaan AWS Well-Architected Tool untuk mendokumentasikan dan mengukur beban kerja. Contoh ini menggambarkan, langkah demi langkah, bagaimana mendefinisikan dan mendokumentasikan beban kerja untuk situs web e-commerce ritel.

Topik

- [Langkah 1: Tentukan beban kerja](#)
- [Langkah 2: Dokumentasikan status beban kerja](#)
- [Langkah 3: Tinjau rencana perbaikan](#)
- [Langkah 4: Lakukan perbaikan dan ukur kemajuan](#)

Langkah 1: Tentukan beban kerja

Anda mulai dengan mendefinisikan beban kerja. Ada dua cara untuk menentukan beban kerja. Dalam tutorial ini, kita tidak mendefinisikan beban kerja dari template review. Untuk detail selengkapnya tentang mendefinisikan beban kerja dari template ulasan, lihat [the section called “Menentukan beban kerja”](#)

Untuk menentukan beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka AWS Well-Architected Tool konsol di <https://console.aws.amazon.com/wellarchitected/>.

Note

Pengguna yang mendokumentasikan status beban kerja harus memiliki [izin akses penuh](#). AWS WA Tool

2. Di bagian Tentukan beban kerja, pilih Tentukan beban kerja.
3. Di kotak Nama, masukkan **Retail Website - North America** sebagai nama beban kerja.
4. Di kotak Deskripsi, masukkan deskripsi untuk beban kerja.
5. Di kotak Pemilik tinjau, masukkan nama orang yang bertanggung jawab atas proses peninjauan beban kerja.

6. Di kotak Lingkungan, tunjukkan bahwa beban kerja berada di lingkungan produksi.
7. Beban kerja kami berjalan pada keduanya AWS dan di pusat data lokal kami:
 - a. Pilih Region AWS, dan pilih dua Wilayah di Amerika Utara tempat beban kerja berjalan.
 - b. Juga pilih AWS Non-region, dan masukkan nama untuk pusat data lokal.
8. IDKotak Akun bersifat opsional. Jangan kaitkan apa pun Akun AWS dengan beban kerja ini.
9. Kotak Aplikasi adalah opsional. Jangan masukkan Aplikasi ARN untuk beban kerja ini.
10. Kotak diagram Arsitektur adalah opsional. Jangan mengaitkan diagram arsitektur dengan beban kerja ini.
11. Jenis Industri dan kotak Industri bersifat opsional dan tidak ditentukan untuk beban kerja ini.
12. Trusted AdvisorBagian ini opsional. Jangan Aktifkan Trusted Advisor Support untuk beban kerja ini.
13. Bagian Jira adalah opsional. Jangan Mengganti pengaturan level akun di bagian JIRA untuk beban kerja ini.
14. Untuk contoh ini, jangan terapkan tag apa pun ke beban kerja. Pilih Berikutnya.
15. Langkah Terapkan profil adalah opsional. Jangan menerapkan profil untuk beban kerja ini. Pilih Berikutnya.
16. Untuk contoh ini, terapkan lensa AWS Well-Architected Framework, yang dipilih secara otomatis. Pilih Tentukan beban kerja untuk menyimpan nilai-nilai ini dan menentukan beban kerja.
17. Setelah beban kerja ditentukan, pilih Mulai meninjau untuk mulai mendokumentasikan status beban kerja.

Langkah 2: Dokumentasikan status beban kerja

Untuk mendokumentasikan keadaan beban kerja, Anda disajikan dengan pertanyaan untuk lensa yang dipilih yang mencakup pilar Kerangka Kerja AWS Well-Architected: keunggulan operasional, keamanan, keandalan, efisiensi kinerja, optimalisasi biaya, dan keberlanjutan.

Untuk setiap pertanyaan, pilih praktik terbaik yang Anda ikuti dari daftar yang disediakan. Jika Anda memerlukan detail tentang praktik terbaik, pilih Info dan lihat informasi dan sumber daya tambahan di panel kanan.

[Pilih Minta ahli untuk mengakses komunitas AWS re:Post yang didedikasikan untuk AWS Well-Architected.](#) Di komunitas ini, Anda dapat mengajukan pertanyaan terkait dengan merancang, membangun, menerapkan, dan mengoperasikan beban kerja. AWS

Operational Excellence 0/11

Well-Architected Tool > Workloads > Retail Website > AWS Well-Architected Framework > Review workload

AWS Well-Architected Framework

Add a link to your architectural design

OPS 1. How do you determine what your priorities are? [Info](#) [Ask an expert](#)

Everyone needs to understand their part in enabling business success. Have shared goals in order to set priorities for resources. This will maximize the benefits of your efforts.

Question does not apply to this workload [Info](#)

Select from the following

- Evaluate external customer needs [Info](#)
- Evaluate internal customer needs [Info](#)
- Evaluate governance requirements [Info](#)
- Evaluate compliance requirements [Info](#)
- Evaluate threat landscape [Info](#)
- Evaluate tradeoffs [Info](#)
- Manage benefits and risks [Info](#)
- None of these [Info](#)

► Mark best practice(s) that don't apply to this workload

Notes - optional

2084 characters remaining

[Save and exit](#) [Next](#)

Helpful resources [Ask an expert](#)

[AWS Support](#)
[AWS Cloud Compliance](#)

Evaluate external customer needs
Involve key stakeholders, including business, development, and [operations](#) teams, to determine where to focus efforts on external customer needs. This will ensure that you have a thorough understanding of the [operations](#) support that is required to achieve your desired business outcomes.

Evaluate internal customer needs
Involve key stakeholders, including business, development, and [operations](#) teams, when determining where to focus efforts on internal customer needs. This will ensure that you have a thorough understanding of the [operations](#) support that is required to achieve business outcomes.

Evaluate governance requirements
Ensure that you are aware of guidelines or obligations defined by your organization that may mandate or emphasize specific focus. Evaluate internal factors, such as organization policy, standards, and requirements. Validate that you have mechanisms to identify changes to governance. If no governance requirements are identified, ensure that you have applied due diligence to this determination.

Evaluate compliance requirements
Evaluate external factors, such as regulatory compliance requirements and industry standards, to ensure that you are aware of guidelines or obligations that may mandate or emphasize specific focus. If no compliance requirements are identified, ensure that you apply due diligence to this determination.

Evaluate threat landscape
Evaluate threats to the business (for example, competition, business risk and liabilities, operational risks, and information [security](#) threats) and maintain current information in a risk registry. Include the

1. Pilih Berikutnya untuk melanjutkan ke pertanyaan berikutnya. Anda dapat menggunakan panel kiri untuk menavigasi ke pertanyaan yang berbeda di pilar yang sama atau ke pertanyaan di pilar yang berbeda.
2. Jika Anda memilih Pertanyaan tidak berlaku untuk beban kerja ini atau Tidak satupun dari ini, AWS sarankan Anda menyertakan alasannya di kotak Catatan. Catatan ini disertakan sebagai bagian dari laporan beban kerja dan dapat membantu di masa depan karena perubahan dilakukan pada beban kerja.

Note

Secara opsional, Anda dapat menandai satu atau lebih praktik terbaik individu sebagai tidak berlaku. Pilih Tandai praktik terbaik yang tidak berlaku untuk beban kerja ini dan

pilih praktik terbaik yang tidak berlaku. Anda dapat memilih alasan secara opsional dan memberikan detail tambahan. Ulangi untuk setiap praktik terbaik yang tidak berlaku.

None of these [Info](#)

▼ **Mark best practice(s) that don't apply to this workload**

If one of the best practices within this question does not apply to your workload, you can mark it as not applicable. You can also choose a reason and provide additional notes for documentation.

Evaluate external customer needs [Info](#)

Select reason (optional) ▼

Provide further details (optional)

250 characters remaining

Evaluate internal customer needs [Info](#)

Out of Scope ▼

Internal customer needs to be addressed in following release

190 characters remaining

Evaluate governance requirements [Info](#)

Select reason (optional) ▼

Provide further details (optional)

Note

Anda dapat menjeda proses ini kapan saja dengan memilih Simpan dan keluar. Untuk melanjutkan nanti, buka AWS WA Tool konsol dan pilih Beban kerja di panel navigasi kiri.

3. Pilih nama beban kerja untuk membuka halaman detail beban kerja.
4. Pilih Lanjutkan meninjau dan kemudian arahkan ke tempat yang Anda tinggalkan.
5. Setelah Anda menyelesaikan semua pertanyaan, halaman ikhtisar untuk beban kerja muncul. Anda dapat meninjau detail ini sekarang atau menavigasi ke sana nanti dengan memilih Beban kerja di panel navigasi kiri dan memilih nama beban kerja.

Setelah mendokumentasikan status beban kerja Anda untuk pertama kalinya, Anda harus menyimpan tonggak sejarah dan menghasilkan laporan beban kerja.

Tonggak sejarah menangkap keadaan beban kerja saat ini dan memungkinkan Anda mengukur kemajuan saat Anda membuat perubahan berdasarkan rencana peningkatan Anda.

Dari halaman detail beban kerja:

1. Di bagian Ikhtisar beban kerja, pilih tombol Simpan tonggak sejarah.
2. Masukkan **Version 1.0 - initial review** sebagai nama Milestone.
3. Pilih Simpan.
4. Untuk menghasilkan laporan beban kerja, pilih lensa yang diinginkan dan pilih Hasilkan laporan dan PDF file dibuat. File ini berisi status beban kerja, jumlah risiko yang diidentifikasi, dan daftar perbaikan yang disarankan.

Langkah 3: Tinjau rencana perbaikan

Berdasarkan praktik terbaik yang dipilih, AWS WA Tool mengidentifikasi area dengan risiko tinggi dan menengah yang diukur dengan Lensa Kerangka AWS Well-Architected.

Untuk meninjau rencana perbaikan:

1. Pilih AWS Well-Architected Framework dari bagian Lenses pada halaman Ikhtisar.
2. Kemudian pilih Rencana perbaikan.

Untuk contoh beban kerja khusus ini, tiga masalah risiko tinggi dan satu masalah risiko menengah diidentifikasi oleh AWS Well-Architected Framework Lens.

AWS Well-Architected Framework Lens

Overview

Improvement plan

Improvement plan overview

Risks

⊗ High risk	3
⚠ Medium risk	1

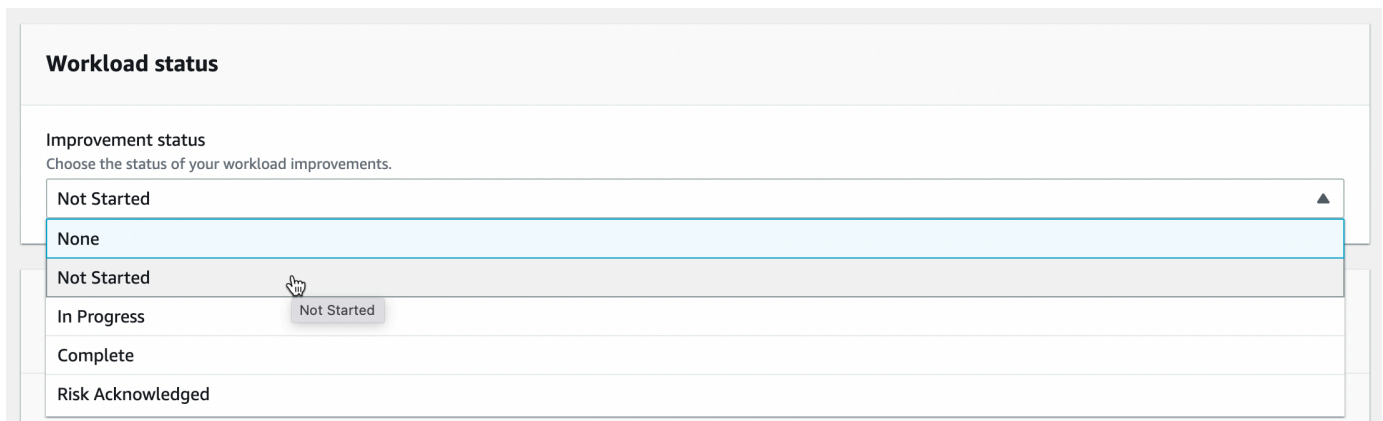
Improvement items

< 1 >

Perbarui status Peningkatan beban kerja untuk menunjukkan bahwa peningkatan beban kerja belum dimulai.

Untuk mengubah status Perbaikan:

1. Dari rencana Improvement, klik nama workload (**Retail Website - North America**) di remah roti di bagian atas halaman.
2. Klik pada tab Properties.
3. Arahkan ke bagian Status beban kerja dan pilih Tidak Dimulai dari daftar dropdown.



4. Arahkan kembali ke rencana Improvement dari tab Properties dengan mengklik tab Overview dan kemudian mengklik link AWS Well-Architected Framework di bagian Lenses. Kemudian klik pada tab Perbaikan rencana di bagian atas halaman.

Bagian Item perbaikan menunjukkan item perbaikan yang direkomendasikan yang diidentifikasi dalam beban kerja. Pertanyaan disusun berdasarkan prioritas pilar yang ditetapkan, dengan masalah risiko tinggi yang terdaftar terlebih dahulu diikuti oleh masalah risiko menengah.

Perluas Item perbaikan yang disarankan untuk menunjukkan praktik terbaik untuk sebuah pertanyaan. Setiap tindakan perbaikan yang direkomendasikan terkait dengan panduan ahli terperinci untuk membantu Anda menghilangkan, atau setidaknya mengurangi, risiko yang diidentifikasi.

Jika profil dikaitkan dengan beban kerja, hitungan risiko yang diprioritaskan ditampilkan di bagian Ikhtisar rencana perbaikan, dan Anda dapat memfilter daftar item Peningkatan dengan memilih Diprioritaskan berdasarkan profil. Daftar item perbaikan menampilkan label Prioritas.

Langkah 4: Lakukan perbaikan dan ukur kemajuan

Sebagai bagian dari rencana peningkatan ini, salah satu masalah berisiko tinggi diatasi dengan menambahkan Amazon CloudWatch dan AWS Auto Scaling dukungan untuk beban kerja.

Dari bagian Item Perbaikan:

1. Pilih pertanyaan terkait dan perbarui praktik terbaik yang dipilih untuk mencerminkan perubahan. Catatan ditambahkan untuk mencatat peningkatan.
2. Kemudian pilih Simpan dan keluar untuk memperbarui status beban kerja.
3. Setelah melakukan perubahan, Anda dapat kembali ke rencana Peningkatan dan melihat efek perubahan tersebut terhadap beban kerja. Dalam contoh ini, tindakan tersebut telah meningkatkan profil risiko — mengurangi jumlah masalah risiko tinggi dari tiga menjadi hanya satu.

Well-Architected Tool > Workloads > Retail Website - North America



Retail Website - North America

Delete workload

Review | **Improvement plan** | Milestones | Properties

Improvement plan overview

Risks

 High risk	1
 Medium risk	2

Anda dapat menyimpan tonggak sejarah pada saat ini, dan kemudian pergi ke Milestones untuk melihat bagaimana beban kerja telah meningkat.

Peninjauan Kerangka Kerja Well-Architected (WAFR)

[Kerangka Kerja Well-Architected](#) menjelaskan konsep-konsep kunci dan prinsip-prinsip desain untuk membuat dan menjalankan beban kerja di cloud. Kerangka kerja ini akan membantu Anda mengetahui kelebihan dan kekurangan dari keputusan yang Anda ambil saat membangun sistem di AWS. Dengan Kerangka Kerja ini, Anda akan dapat mempelajari praktik-praktik terbaik arsitektur untuk merancang dan mengoperasikan aplikasi yang andal, aman, efisien, hemat biaya, dan ramah lingkungan.

Selama Peninjauan Kerangka Kerja Well-Architected (WAFR), Anda akan menjawab serangkaian pertanyaan dasar untuk mempelajari seberapa selaras arsitektur Anda dengan praktik terbaik cloud dan menerima panduan untuk menerapkan peningkatan.

Fase WAFR

Proses WAFR terdiri dari tiga fase utama:

- [Persiapan](#): Siapkan kesuksesan dengan perencanaan yang tepat dan penyelarasan dengan para pemangku kepentingan
- [Peninjauan](#): Melakukan penilaian aktual berdasarkan praktik terbaik AWS
- [Peningkatan](#): Ubah temuan menjadi peningkatan yang dapat ditindaklanjuti untuk beban kerja Anda

Dokumen ini memandu Anda melalui tiga fase, dengan memverifikasi bahwa Anda memiliki persiapan yang cukup untuk mendapatkan nilai maksimal dari fase peninjauan. Kami juga memandu Anda untuk mengubah temuan WAFR Anda menjadi peningkatan yang dapat ditindaklanjuti untuk beban kerja Anda.

Bersiap untuk WAFR

Penting untuk tidak terburu-buru dalam menjalankan Peninjauan Kerangka Kerja Well-Architected (WAFR) tanpa persiapan yang memadai. Terburu-buru dapat menyebabkan prosesnya memakan waktu lebih lama dari yang diharapkan, sehingga memberikan hasil yang kurang menguntungkan dan membuat pengambilan tindakan menjadi lebih sulit.

Peninjauan arsitektur menimbulkan beban manusia yang terkait. Jika grup atau anggota tim dapat mempersiapkan di awal, hal ini akan menghemat waktu di tahap selanjutnya, di mana lebih banyak

orang akan diminta menghadiri sesi. Hal ini juga dapat menghilangkan kebutuhan untuk diskusi kelompok yang lebih besar melalui perencanaan sesi yang lebih baik dan teknik komunikasi asinkron.

Memiliki definisi yang jelas tentang siapa pemilik beban kerja, bagaimana beban kerja dirancang, tujuannya, dan keselarasannya dengan hasil bisnis organisasi Anda dapat membantu Anda mencapai hasil yang lebih baik selama fase peninjauan dan peningkatan.

Fase persiapan terdiri dari tiga elemen utama:

1. Beban kerja dan cakupan
2. Orang dan budaya
3. Dokumentasi dan infrastruktur

Beban kerja dan cakupan

Menurut [Kerangka Kerja AWS Well-Architected](#):

Beban kerja adalah kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti proses backend atau aplikasi yang berinteraksi dengan pelanggan. Beban kerja mungkin terdiri dari subkumpulan sumber daya dalam satu Akun AWS atau merupakan kumpulan beberapa sumber daya yang mencakup beberapa. Akun AWS Bisnis kecil mungkin hanya memiliki beberapa beban kerja, sedangkan perusahaan besar mungkin memiliki ribuan.

Beban kerja itu lebih dari sekadar layanan atau sumber daya cloud. Beban kerja juga mencakup orang, tim, proses, dan runbook, bersama dengan teknologi dan infrastruktur yang memberikan nilai bisnis. Sebelum menjalankan WAFR, investasikan waktu untuk memahami dan mendokumentasikan komponen beban kerja Anda. Hal ini dapat membantu Anda menghemat waktu selama fase peninjauan.

Memilih beban kerja untuk WAFR

Untuk mempersiapkan beban kerja WAFR, diskusikan pertanyaan-pertanyaan berikut dengan tim:

- Siapa pemilik beban kerja ini? Siapa yang bertanggung jawab jika gangguan beban kerja ini berdampak pada bisnis?
- Apa tujuan dari beban kerja ini? Apakah ada analitik untuk bisnis? Apakah beban kerja ini memiliki sandbox, pelatihan, dan pencatatan log?
- Apakah beban kerja ini harus ada? Apa yang terjadi jika Anda mematikannya?

- Apakah beban kerja ini berinteraksi dengan pelanggan atau internal?
- Apakah beban kerja ini untuk produksi atau nonproduksi?
- Pada fase apa beban kerja ini berada dalam siklus hidupnya?
- Apa dampaknya jika beban kerja ini mengalami gangguan?
- Apa batas-batas beban kerja ini?
- Dependensi apa yang dimiliki beban kerja ini?

Anda harus dapat dengan jelas menjawab sebagian besar pertanyaan ini ketika mengevaluasi beban kerja Anda sebelum melanjutkan dengan WAFR.

Apa cakupan peninjauannya?

Meskipun pada akhirnya WAFR mencakup [semua pilar Kerangka Kerja](#), kita dapat mengidentifikasi kompromi dan memahami konteksnya sebelum membuat keputusan. Cara yang baik untuk memulai adalah fokus pada pilar yang diprioritaskan atau area tertentu dari beban kerja.

Mendefinisikan proses peninjauan yang lebih besar, memberikan beberapa hasil yang dapat ditindaklanjuti, dan iterasi akan membantu Anda menghasilkan lebih banyak nilai untuk beban kerja dan bisnis.

Pertimbangkan pendekatan bertahap:

1. Identifikasi dua hingga tiga pilar utama yang paling relevan dengan konteks bisnis dan teknis saat ini
2. Tunjukkan nilai beban kerja Anda dalam pilar-pilar ini
3. Setelah Anda mendapatkan hasil yang memuaskan, iterasikan dengan lebih banyak pilar

Untuk mengurangi cakupan lebih lanjut, gunakan lensa yang dirancang khusus untuk beban kerja Anda.

Orang dan budaya

Setiap beban kerja membutuhkan pemilik, dan banyak orang dan tim mungkin terlibat dalam siklus hidup beban kerja. Namun, sebelum menjalankan WAFR, tentukan single-threaded owner (STO) untuk beban kerja.

Orang ini harus dapat membuat keputusan serta mengontrol anggaran, jumlah karyawan, dan peta panduan. Contoh peran ini adalah pemilik produk, manajer produk, kepala arsitek, atau manajer teknik.

Pada akhirnya, peran ini bertanggung jawab jika beban kerja tidak lagi berfungsi sebagaimana dimaksud.

Sangat penting untuk menjalankan WAFR dengan satu STO untuk meningkatkan hasil Anda. Misalnya, Anda mungkin menemukan item peningkatan untuk beban kerja, tetapi kurang berhasil dalam memprioritaskannya pada peta panduan produk. Atau, Anda mungkin kesulitan mendapatkan dana atau sumber daya untuk melaksanakan pekerjaan.

Hal ini sering mengakibatkan terkumpulnya daftar item backlog yang tidak dapat dicapai. STO membantu Anda menghindari hasil ini karena mereka adalah pemilik WAFR dan berdedikasi terhadap prosesnya.

Pemangku kepentingan yang diperlukan

STO tidak dapat menjawab semua pertanyaan. Banyak orang dan tim terlibat dalam merancang, mengembangkan, mengamankan, atau mengoperasikan beban kerja. Tergantung pada organisasi dan ukuran beban kerja, jumlah pemangku kepentingan dan tim yang terlibat akan bervariasi.

Pertimbangkan pertanyaan-pertanyaan berikut mengenai pemangku kepentingan:

1. Siapa yang perlu hadir untuk menjawab setiap kategori pertanyaan?
2. Pemangku kepentingan mana yang harus hadir di bagian tertentu dari WAFR?
3. Bagaimana cara Anda menginformasikan pertanyaannya kepada berbagai pemangku kepentingan di awal?

Sponsor pilar

Kerangka Kerja Well-Architected terdiri dari [enam pilar](#): Meskipun menentukan STO itu sangat penting, sama pentingnya untuk mendapatkan dukungan dari sponsor atau penggiat khusus pilar guna mempercepat dan meningkatkan nilai proses WAFR.

Tentukan sponsor pilar atau penggiat yang dapat:

- Menghadiri bagian tertentu dari WAFR untuk memberikan informasi atau panduan
- Menjadi pemilik atas hasil untuk bidang khusus mereka

- Mendefinisikan, memengaruhi, dan mengomunikasikan perubahan strategis lintas organisasi

Apakah organisasi Anda memiliki Pusat Keunggulan Cloud atau Komunitas Praktisi Cloud? Mulailah dari yang kecil dan kumpulkan sekelompok orang berpikiran sama yang dapat saling mendukung dengan diskusi dan peningkatan kesehatan arsitektur.

Ciptakan ruang yang aman

Mengembangkan budaya organisasi yang sehat sangat penting untuk diskusi yang sehat dan produktif tentang pilihan teknologi. Kelompok orang yang terlibat dalam WAFR mungkin masih baru atau sudah lama mengenal beban kerja, memiliki masa jabatan dan senioritas yang berbeda, atau terlibat sebagai partner dan pihak ketiga. Sangat penting untuk memelihara percakapan yang sehat dan penuh hormat tentang beban kerja untuk memperbesar kemungkinan peningkatan yang bertahan lama dan bermanfaat.

Tetapkan niat positif dari awal dan tekankan kembali di sepanjang prosesnya guna mempertahankan keselarasan dan fokus untuk menemukan peluang peningkatan. Teknologi dan praktik terbaik terus berubah sehingga WAFR harus dianggap sebagai peluang untuk menemukan peningkatan.

WAFR bukanlah audit. Meskipun temuan dapat membantu Anda memenuhi berbagai standar kepatuhan yang berbeda, prosesnya tidak disediakan untuk “menilai” beban kerja. Fokuslah pada peningkatan kesehatan arsitektur.

WAFR adalah kesempatan untuk bertanya “apa kondisi saat ini?” dan untuk mendapatkan gambaran beban kerja pada titik waktu tertentu. Kemudian, Anda dapat menggunakan temuan untuk membuat keputusan berdasarkan informasi guna menjawab “apa sasaran kita?”

Peningkatan arsitektur adalah perjalanan yang dipandu oleh AWS Well-Architected. Pertimbangkan pertanyaan-pertanyaan berikut saat Anda memulai proses WAFR Anda:

1. Mengapa Anda menjalankan WAFR?
2. Apa yang Anda harapkan dari proses ini?
3. Bagaimana pengalaman ini akan bermanfaat bagi semua orang?
4. Apa kondisi Anda sekarang, dan apa sasaran Anda?

Sumber daya

- [Postingan Blog tentang Akuntabilitas](#)

- [Tim Dua Piza Amazon](#)

Dokumentasi dan infrastruktur

Saat menjalankan WAFR, Anda mungkin menemukan bahwa untuk banyak praktik terbaik yang Anda ikuti, Anda akan memiliki proses yang terdokumentasi, prosedur operasi standar (SOP), runbook, atau buku pedoman. Selama WAFR, catat informasi dan konteks di bidang catatan dalam Alat Well-Architected (Alat WA). Anda dapat menghemat waktu selama peninjauan dengan mengumpulkan semua artefak dokumentasi relevan yang berhubungan dengan beban kerja sebelumnya.

Pertimbangkan pertanyaan-pertanyaan berikut saat Anda mengkaji dokumentasi Anda:

- Dokumentasi apa yang ada tentang beban kerja?
- Dokumentasi apa yang tidak ada?
- Alat apa yang akan digunakan untuk membuat dan menyimpan artefak ini?
- Siapa yang akan terlibat dalam pembuatan dan pemeliharaan artefak ini?

Beberapa contoh dokumentasi tentang beban kerja Anda meliputi:

- Halaman wiki beban kerja
- Diagram arsitektur
- Catatan keputusan arsitektur (ADR)
- Prosedur operasi standar (SOP)
- Repositori infrastruktur sebagai kode (IaC)
- Topologi jaringan
- Buku pedoman dan runbook
- Struktur organisasi atau tim
- Dokumentasi strategi multiakun
- Konfigurasi penyedia identitas pusat
- Konfigurasi solusi pemantauan pusat
- Dokumentasi untuk beban kerja dependen
- Panduan referensi API
- Versi pustaka perangkat lunak
- Proses dan riwayat koreksi kesalahan (COE)
- Strategi chaos engineering
- Detail tim pengujian beban

- Model ancaman
- Rapat retrospektif tim
- Dokumen game day

Anti-pola

Jika tidak ada sumber daya ini, Anda masih dapat menjalankan WAFR sebagai mekanisme penemuan. Namun, prosesnya bisa memakan waktu lebih lama tanpa artefak-artefak ini. Membuat aset dokumentasi dapat menjadi langkah pertama menuju peningkatan kesehatan arsitektur.

Penemuan beban kerja

Sulit untuk meninjau arsitektur secara efisien tanpa mengetahui komponen dan sumber dayanya. Beban kerja warisan sering berkembang dari waktu ke waktu atau berganti kepemilikan, dan mungkin tidak didefinisikan menggunakan alat infrastruktur sebagai kode (IaC) seperti AWS CloudFormation, AWS CDK, atau Terraform.

Sebelum membahas peningkatan, pahami berbagai komponen arsitektur yang berbeda dari beban kerja dan dependensinya, serta buat representasi visual untuk memberikan pemahaman bersama.

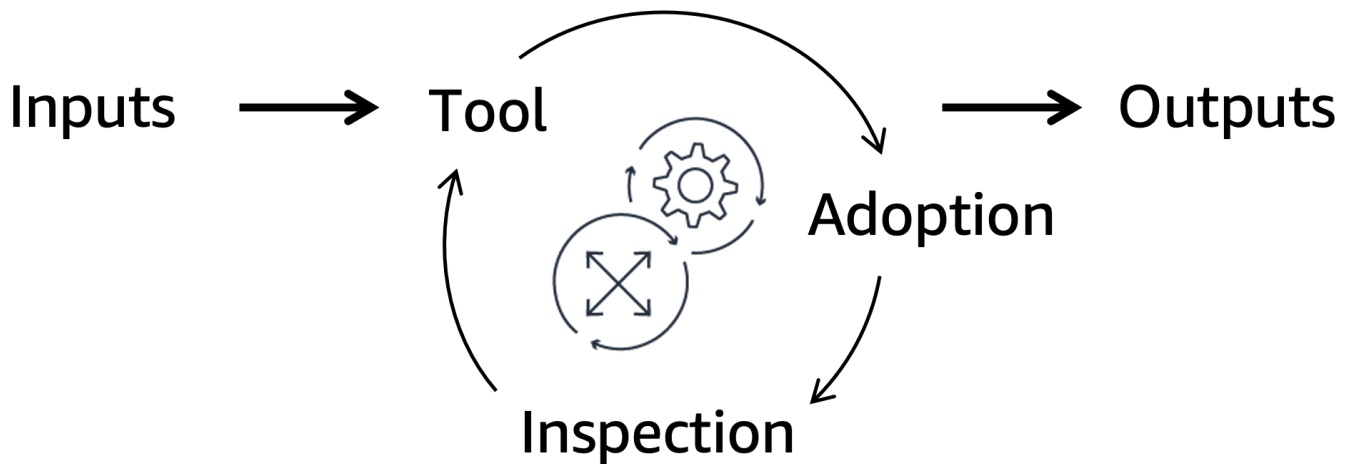
Ada banyak alat penemuan dan diagram otomatis pihak ketiga yang tersedia langsung dari vendor perangkat lunak, dari [AWS Marketplace](#), atau sebagai solusi sumber terbuka.

Sumber daya

- [Diagram Arsitektur Referensi AWS](#)
- [Proses Catatan Keputusan Arsitektur](#)
- [Beranda GitHub ADR](#)
- [Mengapa Anda harus mengembangkan koreksi kesalahan \(COE\)](#)
- [Penemuan Beban Kerja di Solusi AWS](#)

Mekanisme

Mekanisme menggantikan upaya terbaik manusia dengan proses dan alat yang dapat diulang dan dapat diskalakan, yang sering kali otomatis, untuk mencapai hasil yang diinginkan. Mekanisme adalah siklus lengkap di mana Anda membuat alat atau proses, mendorong adopsi, dan memeriksa hasilnya untuk melakukan penyesuaian. Siklus ini mengambil input yang dapat dikontrol dan mentransformasinya menjadi output berkelanjutan untuk mengatasi tantangan bisnis yang berulang.



Sifat siklik dari suatu mekanisme membuatnya paling cocok untuk memecahkan masalah atau peluang yang berulang. WAFR adalah mekanisme dengan alat, proses adopsi, dan proses inspeksi yang semuanya beroperasi dalam sebuah siklus lengkap.

Saat melakukan WAFR untuk beban kerja Anda, Anda mengidentifikasi peluang peningkatan untuk mengembangkan mekanisme lain di organisasi Anda. Hasil dari WAFR seharusnya tidak menjadi perbaikan satu kali untuk satu tim, tetapi harus dibagikan ke banyak tim untuk memberikan nilai maksimal.

Hasil bisnis

Sebelum Anda mulai membuat perubahan pada teknologi, tentukan prioritas bisnis Anda. Akan kurang efektif untuk meninjau arsitektur Anda tanpa pemahaman yang jelas tentang prioritas organisasi Anda. Prioritas ini dapat berfungsi sebagai pedoman untuk membantu Anda mempertahankan keselarasan dan memberikan hasil yang lebih baik.

Hasil bisnis adalah tujuan bisnis utama bernilai tinggi yang terkait dengan strategi organisasi dan didorong oleh umpan balik pelanggan. Hasil bisnis sengaja ditetapkan pada tingkat tinggi sehingga berbagai tim yang berbeda dapat menentukan sasaran yang lebih spesifik untuk mencapainya.

Contoh hasil bisnis umum adalah:

- Memangkas biaya
- Meningkatkan laba
- Meningkatkan kepuasan pelanggan
- Meningkatkan retensi pelanggan
- Meningkatkan retensi karyawan

- Meningkatkan pelestarian lingkungan
- Meningkatkan postur keamanan

Dengan memahami dan melakukan penelusuran mundur dari hasil bisnis organisasi Anda, Anda akan dapat menghemat waktu dengan berfokus pada perubahan teknologi yang dapat membuat dampak paling besar terhadap sasaran organisasi Anda. Hal ini pada gilirannya meningkatkan kepercayaan dari tim kepemimpinan Anda.

Temukan dan diskusikan apa yang menjadi prioritas bisnis saat ini untuk organisasi, unit bisnis, atau tim Anda.

Sumber daya

- [Cara melakukan Peninjauan Kerangka Kerja Well-Architected - Bagian 1](#)

Menjalankan WAFR

Setelah semua persiapan yang diperlukan, sekarang saatnya bagi Anda untuk menjalankan Peninjauan Kerangka Kerja Well-Architected (WAFR). Di bagian ini, kita akan mengkaji kiat dan trik untuk menjadi lebih efisien saat melakukan WAFR Anda.

Sebelum WAFR

Sebelum Anda mulai membahas beban kerja sebagai sebuah kelompok, baca bagian berikut dan diskusikan tata tertib untuk sesi ini. Anda harus memiliki konsensus di grup Anda tentang pelaksanaannya.

Menentukan peran dan tanggung jawab

- Siapa yang memimpin WAFR?
- Siapa yang akan berbagi layar mereka, dan apa yang akan mereka bagikan di sana?
- Siapa yang akan membuat catatan di Alat WA atau format lain?
- Pilar mana yang akan Anda tinjau dan seperti apa urutannya?
- Apakah Anda memiliki orang yang tepat di ruangan untuk menjawab pertanyaan?
- Bagaimana cara Anda akan mendokumentasikan item-item di luar cakupan, dan bagaimana cara Anda akan membuat backlog untuk item-item ini?
- Berapa banyak waktu yang ingin Anda alokasikan untuk setiap bagian atau pilar?
- Apa yang ingin Anda capai dalam waktu yang telah Anda alokasikan?

Kiat peninjauan

Rencanakan rapat tersebut untuk mendokumentasikan titik-titik data tentang pilihan arsitektur beban kerja. Ada beberapa hal yang dapat Anda lakukan untuk membuat bagian WAFR ini semulus mungkin.

1. Komunikasikan niat positif: Tegaskan kembali niat positif WAFR dengan para peserta. Pembahasan kritis tentang pekerjaan bisa jadi sulit, jadi tegaskan kembali bahwa WAFR dilakukan untuk menemukan peluang peningkatan. Tanamkan budaya tidak menyalahkan. Tidak ada menyerang atau membela diri, melainkan diskusi kolaboratif tentang peningkatan arsitektur.
2. Bawa satu orang pendukung: Mengkaji arsitektur beban kerja yang kompleks, mengajukan pertanyaan, memoderasi respons, dan mencatat dapat menyulitkan satu orang. WAFR yang sukses adalah kegiatan tim. Tentukan peran alternatif, sehingga satu orang dapat menjalankan peninjauan, sedangkan yang lain mencatat, memeriksa dokumentasi, dan memantau diskusi.
3. Tetap pada topik: Ketika melakukan percakapan kelompok seputar keputusan arsitektur, biasanya perhatian orang teralihkan. Jika Anda ingin mengefisienkan waktu, pastikan bahwa peserta WAFR dengan hormat saling mengingatkan untuk tetap pada topik. Dokumentasikan konsep dan ide sampingan di tempat terpusat yang dapat diakses kembali selama sesi diskusi mendatang.
4. Buat catatan yang bagus: Hanya dengan mencentang kotak di Alat WA tidak akan memberikan konteks bagi seseorang yang akan meninjau kembali WAFR ini di tahap selanjutnya. Gunakan kotak catatan di Alat WA, atau buat dokumen eksternal yang ditautkan dari kotak catatan WAFR jika Anda melebihi batas karakter. Konteks membantu pihak lain, terutama orang-orang yang baru mengenal beban kerja ini, memahami pekerjaan yang sedang berlangsung dan menentukan apa yang harus diprioritaskan.
5. Jangan fokus pada solusi: Fokuslah pada mendokumentasikan titik-titik data tentang beban kerja daripada solusi. Terlalu banyak fokus pada solusi dapat membuang waktu selama sesi WAFR Anda dan mencegah Anda mendokumentasikan titik-titik data penting. Waktu peserta lain menjadi sia-sia jika Anda melakukan curah pendapat tentang hal-hal di luar cakupan.
6. Fokus pada beban kerja, bukan alat: Orang biasanya membagikan layar mereka yang menampilkan Alat Well-Architected (Alat WA) di Konsol Manajemen AWS. Meskipun dokumentasi data di Alat WA sangat penting, jangan hanya fokus pada alat ini. Fokuskan diskusi Anda pada arsitekturnya. Jaga proses peninjauan ini tetap dalam bentuk percakapan, dan parafrasekan pertanyaan-pertanyaan agar selaras dengan konteksnya.
7. Bagilah diskusi menjadi beberapa bagian: Mungkin sulit untuk meninjau keenam pilar dalam satu rapat. Sebarkan peninjauan ini ke dalam beberapa sesi yang lebih kecil, sehingga memungkinkan pendekatan yang lebih berorientasi topik dan dapat lebih mudah untuk dijadwalkan dengan peserta Anda.

8. Ingatlah untuk mengambil istirahat: Meninjau arsitektur secara menyeluruh dapat melelahkan bagi peserta, dan konsentrasi mereka dapat hilang seiring waktu. Jadwalkan istirahat yang sering selama WAFR. Gunakan waktu peserta dengan cermat, dan izinkan orang untuk meninggalkan rapat jika mereka tidak lagi dibutuhkan.
9. Pikirkan baik-baik tentang kata "mungkin": Jika Anda mendapati bahwa jawaban atas sebuah pertanyaan adalah "mungkin", "kurang lebih", atau "jawabannya akan menyusul", pertimbangkan dengan cermat apakah jawaban sebenarnya adalah "tidak". WAFR bertujuan untuk mendokumentasikan keadaan beban kerja terkini secara jujur, bukan keadaan yang dimaksudkan.
10. Pertimbangkan komprominya: Well-Architected bertujuan untuk membuat kompromi di antara berbagai pilar yang ada. Menjadikan beban kerja lebih tangguh mungkin akan merugikan optimalisasi biaya Anda, atau mengoptimalkan biaya lebih lanjut mungkin akan berdampak pada efek beban kerja Anda bagi lingkungan. Pilar-pilar ditetapkan untuk menyediakan struktur pada pembahasan Anda dan untuk membantu Anda membuat pilihan arsitektur yang tepat.
11. Ketahuilah bahwa tidak ada beban kerja yang sempurna: Beban kerja jarang sempurna dan sering kali tidak perlu sempurna. Hindari mengubah WAFR Anda menjadi latihan untuk membuat semuanya sempurna, dan fokuslah untuk membuat beban kerja berfungsi dengan aman dan efisien sesuai tujuan bisnis yang dimaksudkan.

Menjalankan WAFR

Jalankan WAFR di Akun AWS bersama beban kerja. Anda kemudian dapat membagikan peninjauan beban kerja ke Akun AWS lain.

[Bagikan peninjauan](#) ke akun pusat menggunakan AWS Organizations. Anda kemudian dapat menggunakan [dasbor](#) untuk melihat beban kerja organisasi Anda secara terpusat.

Hal ini dapat membantu Anda mengenali pola risiko dan peningkatan di semua beban kerja Anda. Anda kemudian dapat mengatasi tantangan secara terpusat dengan pendekatan berbasis pola yang dapat dibagikan dan digunakan di banyak akun dan beban kerja.

Akses IAM

Akses AWS WA Tool di Konsol Manajemen AWS memerlukan izin IAM. Tentukan di awal siapa yang membutuhkan akses untuk menghemat waktu pada permulaan sesi WAFR.

Untuk detail selengkapnya, lihat [Memberikan akses untuk pengguna, grup, atau peran ke AWS Well-Architected Tool](#).

Anda dapat menyiapkan [Peran IAM lintas akun](#) untuk memungkinkan pemangku kepentingan eksternal mengakses Alat WA dan mengedit atau melihat peninjauan.

Sumber daya

- [Cara melakukan Peninjauan Kerangka Kerja Well-Architected - Bagian 2](#)

Meningkatkan beban kerja Anda

Pada titik ini, Anda telah mempersiapkan WAFR, menyelesaikan peninjauan, dan menilai beban kerja Anda berdasarkan praktik terbaik AWS.

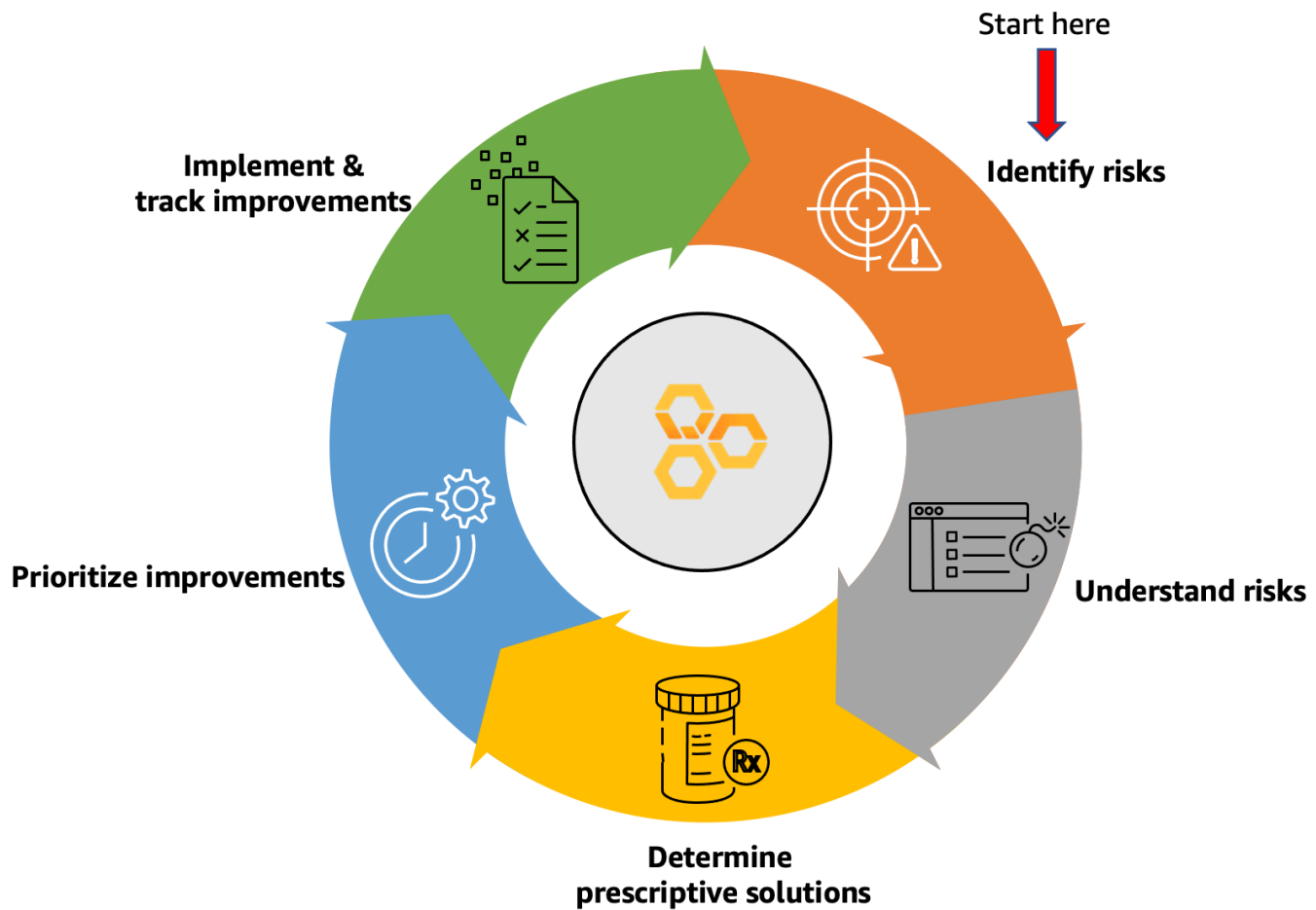
Output dari WAFR akan mengidentifikasi risiko arsitektur berdasarkan jawaban yang didokumentasikan selama peninjauan. Risiko-risiko ini dikategorikan sebagai masalah risiko tinggi (HRI) dan masalah risiko sedang (MRI).

Selama fase terakhir, Anda akan membuat rencana peningkatan yang terdiri dari pembuatan daftar risiko, pemahaman dampaknya terhadap bisnis Anda, identifikasi solusi, dan implementasi solusi tersebut sesuai dengan prioritas organisasi Anda.

Bagian berikut memberikan panduan yang mendetail untuk proses peningkatan beban kerja:

- Identifikasi dan pahami risiko
- Tentukan solusi preskriptif
- Prioritaskan peningkatan
- Implementasikan dan lacak peningkatan

Siklus berikut menunjukkan langkah-langkah utama yang termasuk dalam fase peningkatan dari WAFR.



Identifikasi dan pahami risiko

Lihat risiko yang teridentifikasi sebagai peluang peningkatan.

Ada dua kategori risiko dalam konteks WAFR: masalah risiko tinggi (HRI) dan masalah risiko sedang (MRI).

- **Masalah Risiko Tinggi (HRI):** Pilihan arsitektur dan operasional yang dapat menyebabkan dampak negatif yang signifikan terhadap bisnis. Praktik risiko tinggi dianggap sebagai masalah dasar yang harus dilakukan dalam sebuah pilar. Praktik ini dapat memengaruhi operasi organisasi, aset, dan individu. Salah satu contoh HRI dari pilar keamanan adalah tidak mengamankan Akun AWS Anda.
- **Masalah risiko sedang (MRI):** Pilihan yang juga dapat berdampak negatif pada bisnis Anda, tetapi pada tingkat yang lebih rendah daripada HRI. Praktik terbaik risiko sedang merupakan praktik pendukung yang secara substansial dapat meningkatkan beban kerja. Contoh MRI pada pilar keamanan adalah tidak mengaudit dan merotasi kredensial secara berkala.

Membuat laporan

Langkah pertama untuk mengidentifikasi HRI dan MRI secara visual adalah membuat laporan yang menunjukkan risiko untuk setiap beban kerja yang Anda tinjau.

[Dasbor AWS Well-Architected Tool \(Alat AWS WA\)](#) menyediakan akses ke beban kerja Anda serta HRI dan MRI terkait. Anda juga dapat menyertakan beban kerja yang telah dibagikan kepada Anda. Dengan menggunakan dasbor, Anda dapat memfilter masalah berdasarkan beban kerja, pilar, atau tingkat keparahan (tinggi atau sedang).

Di halaman dasbor, Anda dapat melihat daftar HRI dan MRI yang difilter berdasarkan pilar atau tingkat keparahan. Setelah item peningkatan dipilih, Anda akan diarahkan langsung ke praktik terbaik yang terkait dengannya dari Kerangka Kerja Well-Architected. Dari sana, Anda dapat membaca tentang tindakan yang disarankan yang perlu diambil untuk memulihkan masalah bersama dengan sumber daya yang diperlukan.

Anda dapat menggabungkan semua temuan ini dalam satu laporan dengan memilih [Buat laporan](#) dari Dasbor Alat WA.

Kami merekomendasikan untuk mengirim email rekap ke peserta WAFR bersama dengan laporan, serta merangkum temuan utama dan rencana peningkatan yang disarankan agar mempersiapkan mereka untuk langkah berikutnya.

Mengelola risiko

Untuk mengelola risiko secara efektif, penting untuk menentukan risiko dan tingkat risiko yang dapat diterima. Dengan analisis risiko, kaji apa masalah potensial dan bagaimana cara mengetahui apakah itu masalah.

Ada dua metode utama untuk melakukan penilaian risiko:

- Kuantitatif: Menggunakan data objektif tertimbang untuk menilai dampak risiko dalam hal kelebihan biaya, konsumsi sumber daya, dan penundaan jadwal.
- Kualitatif: Menggunakan data subjektif yang tidak terikat dengan nilai aktual biaya atau manfaat untuk mengukur probabilitas dan dampak keseluruhan.

Dalam beberapa kasus, Anda mungkin akhirnya menggunakan pendekatan campuran yang menggabungkan aspek terbaik dari kedua pendekatan ini untuk menilai dampak risiko.

Saat mengevaluasi tingkat risiko berdasarkan definisi HRI dan MRI, pertimbangkan untuk mengajukan pertanyaan berikut:

- Apa kemungkinan risiko yang mengakibatkan dampak?
- Apa yang akan menjadi dampak pelanggan?
- Apa yang akan menjadi dampak bisnis sebagai hasilnya?
- Dapatkah risiko dihilangkan seluruhnya atau hanya dimitigasi?
- Siapa yang memiliki risikonya?
- Siapa yang memiliki pekerjaan peningkatan untuk menghilangkan atau memitigasinya?
- Apa probabilitasnya bahwa hasil ini akan terjadi lagi? Apakah hasil ini kemungkinan akan menimbulkan dampak yang sama?
- Dapatkah Anda mengidentifikasi hubungan antara kemungkinan hasil dan pola kemunculan kembali?

Dengan meminta para pemangku kepentingan utama atau pemilik bisnis menjawab pertanyaan-pertanyaan ini, Anda akan dapat membuat daftar risiko paling penting untuk difokuskan bersama dengan waktu yang diproyeksikan untuk mengatasinya.

Besaran risiko

Anda dapat menggunakan tabel berikut untuk membantu Anda menentukan besaran risiko:

Kemungkinan x dampak	Kecil sekali (1)	Kecil (2)	Sedang (3)	Besar (4)	Kritis (5)
Hampir pasti (5)	5	10	15	20	25
Cukup mungkin (4)	4	8	12	26	20
Mungkin (3)	3	6	9	12	15
Kurang mungkin (2)	2	4	6	8	10
Tidak mungkin (1)	1	2	3	4	5

Bekerjasamalah sebagai kelompok dalam menangani HRI dan MRI serta risiko yang diakibatkannya pada bisnis. Buat daftar HRI yang perlu ditangani. Beri peringkat risiko berdasarkan kekritisannya untuk menetapkan prioritas.

Tentukan solusi preskriptif

Setelah risiko dan peluang peningkatan dipahami dalam konteks organisasi Anda, bekerjasamalah dengan berbagai tim dalam memitigasinya. Pada fase ini, setiap tim perlu menangani HRI yang ditemukan di area mereka dan menentukan solusi preskriptif untuk mengatasi HRI.

Langkah ini mungkin memerlukan penelitian tambahan, diskusi, atau pengembangan bukti konsep. Penting untuk tidak menghabiskan terlalu banyak waktu untuk mengkaji detail implementasi solusi dalam fase ini. Itu akan dilakukan nanti jika Anda memutuskan bahwa HRI yang dimaksud adalah prioritas.

Tujuan dari langkah ini adalah untuk memahami kompleksitas solusi dan sumber daya apa yang diperlukan sehingga Anda dapat memperhitungkannya saat memprioritaskan tugas berdasarkan waktu, kompleksitas, dan dampak.

Bekerjasamalah sebagai kelompok untuk mengumpulkan daftar solusi yang mungkin untuk HRI. Perhatikan hal-hal yang umum dan jangan masuk ke detail implementasi.

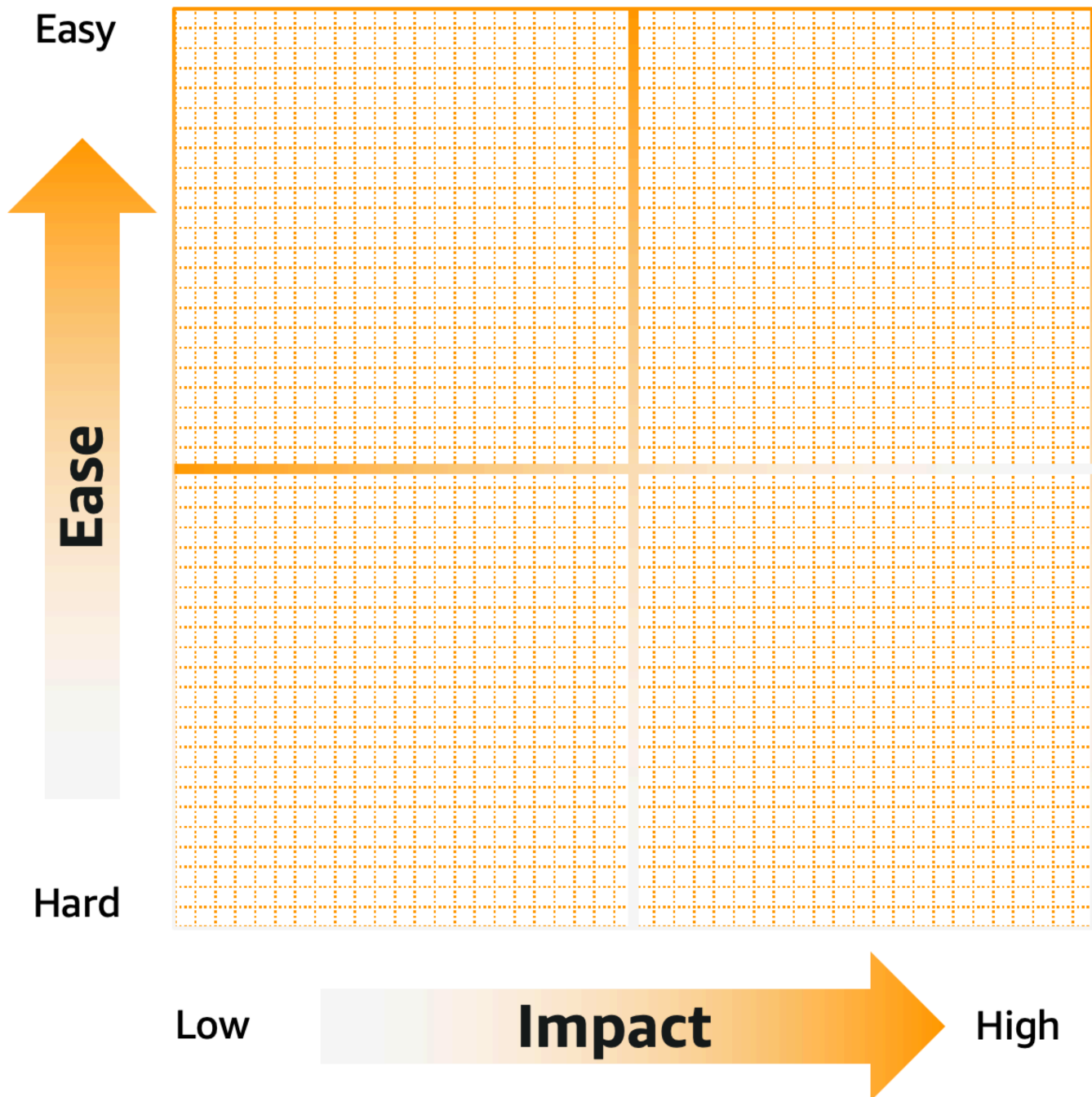
Prioritaskan peningkatan

Tidak ada organisasi yang memiliki waktu dan sumber daya yang tidak terbatas. Mengatasi semua HRI dan MRI yang diidentifikasi sekaligus mungkin bukan cara yang tepat untuk mendapatkan hasil maksimal dari WAFR.

Mulailah dengan sejumlah masalah tertentu yang dapat membuat dampak paling besar pada bisnis dan yang lebih mudah diimplementasikan. Kerjakan solusinya. Lacak peningkatan, lalu iterasikan pendekatan tersebut.

Prioritaskan implementasi

Salah satu pendekatan yang dapat membantu Anda memvisualisasikan prioritas solusi adalah plot bergaya [Eisenhower](#). Ada berbagai cara untuk menggunakan alat ini. Saat mengevaluasi, pertimbangkan tingkat kepentingan peningkatan (berapa banyak nilai yang diberikan ke bisnis Anda) dan upaya yang diperlukan untuk menerapkan peningkatan (waktu yang diperlukan, kompleksitas implementasi, atau jumlah karyawan).



Output dari analisis ini memberikan serangkaian risiko yang memiliki dampak paling besar pada bisnis Anda, tetapi tidak terlalu rumit untuk diimplementasikan. Ini adalah kandidat yang baik untuk mulai diimplementasikan pada iterasi pertama.

Karakteristik solusi

Saat memilih solusi untuk risiko yang diidentifikasi, pertimbangkan hal-hal berikut:

- **Sasaran SMART:** Pikirkan sasaran Specific (Spesifik), Measurable (Terukur), Achievable (Dapat Dicapai), Relevant (Relevan), dan Time-Bound (Terikat Waktu) (SMART).
- **Pemilik:** Untuk setiap solusi, tentukan pemiliknya.
- **Sederhana daripada kompleks:** Solusi kompleks dapat berhasil, tetapi membuat peningkatan lebih sulit untuk diimplementasikan, dan dapat membutuhkan waktu lebih lama untuk dibuat. Pilih kesederhanaan daripada kompleksitas kecuali jika solusi kompleks adalah persyaratan yang tidak dapat dihindari.
- **Buat keputusan pintu dua arah:** Solusi harus dapat diperluas serta dirancang untuk ditingkatkan dan diubah dari waktu ke waktu. Jika memungkinkan, hindari solusi statis yang tidak dapat beradaptasi saat arsitektur Anda berkembang.
- **Solusi berbasis pola target:** Pertimbangkan solusi yang dapat dikodifikasi, digunakan kembali, dan dibagikan kembali. Tidak perlu membuat segalanya dari nol. Akses [Pusat Arsitektur AWS](#) untuk mendapatkan contoh.
- **Bekerja terus-menerus sebagai tim:** Bekerjasamalah sebagai kelompok guna membuat daftar solusi untuk HRI. Prioritaskan solusi dalam matriks Eisenhower.

Implementasikan dan lacak peningkatan

Hasil ideal dari implementasi yang sukses adalah pengurangan HRI dan MRI, yang menghasilkan peningkatan kesehatan arsitektur beban kerja Anda.

Implementasi perbaikan harus dilakukan secara iteratif, menggunakan tonggak pencapaian dalam Alat WA yang mencatat keadaan beban kerja pada titik waktu tertentu. Setiap kali Anda melakukan sesi peninjauan, atau ketika Anda menyelesaikan item peningkatan, simpan tonggak pencapaian untuk mengukur progres seiring waktu.

WAFR dalam Agile

Output dari latihan prioritas WAFR dapat digunakan untuk memprioritaskan tiket untuk sprint dan backlog bagi tim pengembangan. Developer harus dapat memahami dampak implementasi dan memiliki kontribusi terhadap kesehatan arsitektur yang lebih baik. Peningkatan dan pelacakan WAFR dapat diintegrasikan dalam rapat retrospektif Agile.

Rapat retrospektif adalah rapat yang diadakan pada akhir iterasi atau sprint. Selama rapat retrospektif, tim merefleksikan apa yang terjadi dalam iterasi dan mengidentifikasi tindakan untuk peningkatan ke depan. Mekanisme yang ideal adalah menyertakan peninjauan WAFR untuk didiskusikan dan memberdayakan anggota dalam kesehatan arsitektur.

Jadwal

Jadwal untuk langkah-langkah ini bervariasi per organisasi karena setiap organisasi berbeda dan memiliki tantangan unik. Namun, setelah WAFR berhasil dilakukan oleh banyak pelanggan di AWS, kami merekomendasikan fase ini untuk memakan waktu antara 90 dan 180 hari.

Jika daftar HRI dan MRI Anda membutuhkan waktu lebih lama, prioritaskan kembali dan buat daftar yang lebih pendek sehingga Anda dapat mulai mempraktikkan proses untuk mendapatkan beberapa peningkatan. Kemudian, ulangi dengan item Anda yang tersisa.

Jadwal setelah WAFR

Satu hari setelah WAFR:

1. Buat email rekap yang berisi rencana peningkatan, dan rangkum:
 - Siapa yang ikut serta dalam proses peninjauan
 - Temuan penting
 - Jadwal untuk langkah selanjutnya
2. Lampirkan rencana peningkatan
3. Orientasikan tim sesuai rencananya

Dua hingga tiga hari setelah WAFR:

1. Buat rapat prioritas HRI, dan tentukan prioritas HRI:
 - Berdasarkan upaya
 - Berdasarkan dampak
 - Bersama tim yang bertanggung jawab atas beban kerja
2. Berkolaborasi untuk menangani apa yang paling penting bagi bisnis

Satu minggu setelah WAFR:

1. Mulailah rencana peningkatan
2. Pertimbangkan rekomendasi berikut:
 - Durasi: 90 atau 180 hari
 - Identifikasi dan tentukan prioritas HRI

- Kembangkan mitigasi untuk masing-masing HRI
- Coba maksimalkan inisiatif untuk menyelesaikan beberapa HRI

Tugas rutin:

1. Bentuk rutinitas untuk pertemuan lanjutan mengenai rencana peningkatan
2. Tinjau tindakan yang harus diambil untuk meningkatkan beban kerja
3. Pertimbangkan rekomendasi berikut:
 - Tetapkan ekspektasi bagi peserta
 - Kirim mereka tautan pertanyaan di alat WA
 - Lakukan peninjauan lanjutan

Beban kerja

Beban kerja adalah kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti proses backend atau aplikasi yang berinteraksi dengan pelanggan.

Beban kerja mungkin terdiri dari subset sumber daya dalam satu Akun AWS atau merupakan kumpulan beberapa sumber daya yang mencakup beberapa Akun AWS. Bisnis kecil mungkin hanya memiliki beberapa beban kerja, sedangkan perusahaan besar mungkin memiliki ribuan.

Halaman Beban kerja, yang tersedia dari navigasi kiri, memberikan informasi tentang beban kerja Anda dan beban kerja apa pun yang telah dibagikan dengan Anda.

Informasi berikut ditampilkan untuk setiap beban kerja:

Nama

Nama beban kerja.

Pemilik

ID Akun AWS yang memiliki beban kerja.

Pertanyaan yang dijawab

Jumlah pertanyaan yang dijawab.

Risiko tinggi

Jumlah masalah risiko tinggi (HRI) yang diidentifikasi.

Risiko sedang

Jumlah masalah risiko sedang (MRI) yang diidentifikasi.

Status perbaikan

Status perbaikan yang telah Anda tetapkan untuk beban kerja:

- Tidak ada
- Belum Dimulai
- Sedang Berlangsung
- Selesai
- Risiko yang Dikonfirmasi

Terakhir diperbarui

Tanggal dan waktu beban kerja terakhir diperbarui.

Setelah Anda memilih beban kerja dari daftar:

- Untuk meninjau detail beban kerja, pilih Lihat detail.
- Untuk mengubah properti beban kerja, pilih Edit.
- Untuk mengelola pembagian beban kerja dengan Akun AWS lain, pengguna, AWS Organizations, atau unit organisasi (OU), pilih Lihat detail, lalu Pembagian.
- Untuk menghapus beban kerja dan semua titik pencapaiannya, pilih Hapus. Hanya pemilik beban kerja yang dapat menghapusnya.

Warning

Tindakan menghapus beban kerja tidak dapat diurungkan. Semua data yang terkait dengan beban kerja akan dihapus.

Masalah Risiko Tinggi (HRI) dan Masalah Risiko Menengah (MRI)

Masalah risiko tinggi (HRI) yang diidentifikasi di AWS Well-Architected Tool adalah pilihan arsitektur dan operasional yang menurut temuan AWS dapat mengakibatkan dampak negatif yang signifikan terhadap bisnis. HRI ini dapat memengaruhi operasi organisasi, aset, dan individu. Masalah risiko menengah (MRI) juga dapat berdampak negatif pada bisnis, tetapi pada tingkat yang lebih rendah. Masalah-masalah ini didasarkan pada respons Anda di AWS Well-Architected Tool. Praktik terbaik yang sesuai diterapkan secara luas oleh AWS dan pelanggan AWS. Praktik terbaik ini adalah panduan yang ditentukan oleh Kerangka Well-Architected AWS dan lensa.

Note

Ini hanyalah pedoman dan pelanggan harus mengevaluasi serta mengukur dampak yang dihasilkan terhadap bisnis mereka seandainya mereka tidak mengimplementasikan praktik terbaik. Jika ada alasan teknis atau bisnis tertentu yang menghalangi implementasi praktik terbaik pada beban kerja, risikonya mungkin lebih rendah dari yang ditunjukkan. AWS menyarankan agar pelanggan mendokumentasikan alasan-alasan tersebut, serta bagaimana pengaruhnya terhadap praktik terbaik, di dalam catatan beban kerja. Untuk semua HRI dan

MRI yang diidentifikasi, AWS menyarankan agar pelanggan mengimplementasikan praktik terbaik sebagaimana didefinisikan dalam AWS Well-Architected Tool. Jika praktik terbaik telah diimplementasikan, tunjukkan bahwa masalah telah diatasi dengan cara menandai bahwa praktik terbaik telah terpenuhi di AWS Well-Architected Tool. Jika pelanggan memilih untuk tidak mengimplementasikan praktik terbaik, AWS menyarankan agar mereka mendokumentasikan persetujuan tingkat bisnis yang relevan serta alasan mereka tidak mengimplementasikannya.

Menentukan beban kerja di AWS Well-Architected Tool

Ada dua cara untuk menentukan beban kerja. Di halaman Beban kerja di AWS WA Tool, Anda dapat menentukan beban kerja tanpa templat. Atau, di halaman Templat tinjauan, Anda dapat menggunakan templat tinjauan yang sudah ada atau membuat templat baru untuk menentukan beban kerja.

Untuk menentukan beban kerja dari halaman Beban kerja

1. Di panel navigasi kiri, pilih Beban kerja.
2. Pilih dropdown Tentukan beban kerja.
3. Pilih Tentukan beban kerja. Atau, jika Anda telah membuat templat tinjauan dan ingin menentukan beban kerja dari templat tersebut, pilih Tentukan dari templat tinjauan.
4. Ikuti petunjuk di [the section called “Menentukan beban kerja”](#) untuk menentukan properti beban kerja, atau (opsional) menerapkan profil dan lensa.

Untuk menentukan beban kerja dari halaman Templat tinjauan

1. Pilih Templat tinjauan di panel navigasi kiri.
2. Pilih nama templat tinjauan yang sudah ada, atau ikuti petunjuk di [the section called “Membuat template ulasan”](#) untuk membuat templat tinjauan baru.
3. Pilih Tentukan beban kerja dari templat.
4. Ikuti petunjuk di [the section called “Mendefinisikan beban kerja dari template”](#) untuk membuat beban kerja dari templat tinjauan Anda.

Melihat beban kerja di AWS Well-Architected Tool

Anda dapat melihat detail beban kerja yang Anda miliki dan beban kerja yang telah dibagikan kepada Anda.

Untuk melihat beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang akan dilihat dengan salah satu cara berikut:
 - Pilih nama beban kerja.
 - Pilih beban kerja, lalu pilih Lihat detail.

Halaman detail beban kerja akan ditampilkan.

Note

Bidang wajib, Pemilik tinjauan, telah ditambahkan untuk memudahkan Anda mengidentifikasi orang atau grup utama yang bertanggung jawab atas proses peninjauan.

Saat pertama kali melihat beban kerja yang telah ditentukan sebelum bidang ini ditambahkan, Anda akan diberi tahu tentang perubahan ini. Pilih Edit untuk mengisi bidang Pemilik tinjauan dan tidak diperlukan tindakan lebih lanjut.

Pilih Konfirmasi untuk menunda pengisian bidang Pemilik tinjauan. Selama 60 hari ke depan, banner akan ditampilkan untuk mengingatkan Anda bahwa bidang tersebut kosong. Untuk menghilangkan banner tersebut, edit beban kerja Anda dan tentukan Pemilik tinjauan.

Jika Anda tidak mengisi bidang tersebut pada tanggal yang ditentukan, akses Anda ke beban kerja akan dibatasi. Anda tetap dapat melihat beban kerja dan menghapusnya, tetapi Anda tidak dapat mengeditnya, kecuali untuk mengisi bidang Pemilik tinjauan. Akses bersama ke beban kerja tidak terpengaruh saat akses Anda dibatasi.

Mengedit beban kerja di AWS Well-Architected Tool

Anda dapat mengedit detail beban kerja yang Anda miliki.

Untuk mengedit beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang ingin Anda edit, lalu pilih Edit.
4. Buat perubahan Anda pada beban kerja.

Untuk deskripsi tiap bidang, lihat [Menentukan beban kerja di AWS WA Tool](#).

Note

Saat memperbarui beban kerja yang ada, Anda dapat Mengaktifkan Trusted Advisor, yang membuat peran IAM untuk pemilik beban kerja secara otomatis. Pemilik akun terkait untuk beban kerja yang telah mengaktifkan Trusted Advisor harus membuat peran di IAM. Lihat detailnya di [the section called “Mengaktifkan Trusted Advisor di IAM”](#).

5. Pilih Simpan untuk menyimpan perubahan Anda pada beban kerja.

Jika bidang yang wajib diisi kosong atau jika nilai yang ditentukan tidak valid, Anda harus memperbaiki masalahnya sebelum pembaruan beban kerja Anda disimpan.

Berbagi beban kerja di AWS Well-Architected Tool

Anda dapat berbagi beban kerja yang Anda miliki dengan Akun AWS, pengguna, organisasi, dan unit organisasi (OU) lain di AWS Region yang sama.

Note

Anda hanya dapat berbagi beban kerja di AWS Region yang sama. Saat berbagi beban kerja dengan Akun AWS yang lain, jika penerima tidak memiliki izin `wellarchitected:UpdateShareInvitation`, mereka tidak dapat menerima undangan berbagi. Lihat [the section called “Memberikan akses ke AWS WA Tool”](#) untuk contoh kebijakan izin.

Untuk berbagi beban kerja dengan Akun AWS dan pengguna lain

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang Anda miliki dengan salah satu cara berikut:
 - Pilih nama beban kerja.
 - Pilih beban kerja, lalu pilih Lihat detail.
4. Pilih Berbagi. Kemudian pilih Buat dan Buat pembagian ke pengguna atau akun untuk membuat undangan beban kerja.
5. Masukkan ID Akun AWS 12 digit atau ARN pengguna yang akan menerima pembagian beban kerja Anda.
6. Pilih izin yang ingin Anda berikan.

Hanya baca

Menyediakan akses hanya-baca ke beban kerja.


Kontributor

Menyediakan akses pembaruan ke jawaban dan catatannya, dan akses hanya-baca ke sisa beban kerja.

7. Pilih Buat untuk mengirim undangan beban kerja ke Akun AWS atau pengguna yang ditentukan.

Jika undangan beban kerja tidak disetujui dalam waktu tujuh hari, undangan tersebut akan kedaluwarsa secara otomatis.

Jika pengguna dan Akun AWS pengguna sama-sama memiliki undangan beban kerja, undangan beban kerja dengan izin tingkat tertinggi diterapkan ke pengguna.

 Important

Sebelum membagikan beban kerja ke organisasi atau unit organisasi (OU), Anda harus [mengaktifkan akses AWS Organizations](#).

Untuk membagikan beban kerja ke organisasi atau OU

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang Anda miliki dengan salah satu cara berikut:
 - Pilih nama beban kerja.
 - Pilih beban kerja, lalu pilih Lihat detail.
4. Pilih Berbagi. Kemudian pilih Buat dan Buat pembagian ke Organisasi.
5. Di halaman Buat pembagian beban kerja, pilih apakah Anda akan memberikan izin ke seluruh organisasi, atau ke satu atau beberapa OU.
6. Pilih izin yang ingin Anda berikan.

Hanya Baca

Menyediakan akses hanya-baca ke beban kerja.

Kontributor

Menyediakan akses pembaruan ke jawaban dan catatannya, dan akses hanya-baca ke sisa beban kerja.

7. Pilih Buat untuk berbagi beban kerja.

Untuk melihat orang yang memiliki akses ke beban kerja, pilih Berbagi dari halaman [Melihat detail beban kerja di AWS Well-Architected Tool](#).

Agar suatu entitas tidak berbagi beban kerja, lampirkan kebijakan yang menyangkal tindakan `wellarchitected:CreateWorkloadShare`.

Anda juga dapat berbagi lensa kustom yang Anda miliki dengan Akun AWS lain, pengguna, organisasi Anda, dan OU di AWS Region yang sama. Lihat [Membagikan lensa kustom di AWS WA Tool](#) untuk detailnya.

Pertimbangan saat berbagi beban kerja AWS Well-Architected Tool

Beban kerja dapat dibagikan dengan hingga 20 Akun AWS dan pengguna berbeda. Beban kerja hanya dapat dibagikan dengan akun dan pengguna yang berada di AWS Region yang sama dengan beban kerja.

Untuk berbagi beban kerja di Wilayah yang diperkenalkan setelah 20 Maret 2019, Anda dan Akun AWS yang dibagikan harus mengaktifkan Wilayah tersebut di Konsol Manajemen AWS. Untuk informasi lebih lanjut, lihat [Infrastruktur Global AWS](#).

Anda dapat berbagi beban kerja dengan Akun AWS, pengguna individu di akun, atau keduanya. Saat Anda berbagi beban kerja dengan Akun AWS, semua pengguna di akun akan diberi akses ke beban kerja tersebut. Jika yang memerlukan akses hanyalah pengguna tertentu dalam akun, ikuti praktik terbaik untuk memberikan hak akses paling rendah dan bagikan beban kerja secara individual dengan pengguna tersebut.

Jika sebuah Akun AWS dan pengguna di akun tersebut sama-sama memiliki undangan beban kerja, undangan beban kerja dengan izin tingkat tertinggi akan menentukan izin pengguna ke beban kerja. Jika Anda menghapus undangan beban kerja untuk pengguna, akses pengguna akan ditentukan oleh undangan beban kerja untuk Akun AWS. Hapus kedua undangan beban kerja untuk menghapus akses pengguna ke beban kerja.

Sebelum membagikan beban kerja ke sebuah organisasi atau ke satu atau beberapa unit organisasi (OU), Anda harus mengaktifkan akses AWS Organizations.

Jika Anda berbagi beban kerja dengan organisasi dan satu atau beberapa OU, undangan beban kerja dengan izin tingkat tertinggi menentukan izin akun ke beban kerja.

Untuk mengaktifkan berbagi AWS Organizations

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pilih Aktifkan dukungan AWS Organizations.
4. Pilih Simpan pengaturan.

Menghapus akses bersama di AWS Well-Architected Tool

Anda dapat menghapus undangan beban kerja. Menghapus undangan beban kerja akan menghapus akses bersama ke beban kerja.

Untuk menghapus akses bersama ke beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.

2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja dengan salah satu cara berikut:
 - Pilih nama beban kerja.
 - Pilih beban kerja, lalu pilih Lihat detail.
4. Pilih Berbagi.
5. Pilih undangan beban kerja yang akan dihapus dan pilih Hapus.
6. Pilih Hapus untuk mengonfirmasi.

Jika pengguna dan Akun AWS pengguna memiliki undangan beban kerja, Anda harus menghapus kedua undangan beban kerja untuk menghapus izin pengguna ke beban kerja.

Mengubah akses bersama di AWS Well-Architected Tool

Anda dapat mengubah undangan beban kerja yang tertunda atau diterima.

Untuk mengubah akses bersama ke beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang Anda miliki dengan salah satu cara berikut:
 - Pilih nama beban kerja.
 - Pilih beban kerja, lalu pilih Lihat detail.
4. Pilih Berbagi.
5. Pilih undangan beban kerja yang akan diubah lalu pilih Edit.
6. Pilih izin baru yang ingin Anda berikan kepada Akun AWS atau pengguna.

Hanya Baca

Menyediakan akses hanya-baca ke beban kerja.

Kontributor

Menyediakan akses pembaruan ke jawaban dan catatannya, dan akses hanya-baca ke sisa beban kerja.

7. Pilih Simpan.

Jika undangan beban kerja yang diubah tidak diterima dalam waktu tujuh hari, undangan tersebut akan kedaluwarsa secara otomatis.

Menerima dan menolak undangan beban kerja di AWS Well-Architected Tool

Undangan beban kerja adalah permintaan untuk berbagi beban kerja yang dimiliki oleh Akun AWS lain. Jika Anda menerima undangan beban kerja, beban kerja akan ditambahkan ke halaman Beban Kerja dan Dasbor Anda. Jika Anda menolak undangan beban kerja, undangan akan dihapus dari daftar undangan beban kerja.

Anda memiliki waktu tujuh hari untuk menerima undangan beban kerja. Jika Anda tidak menerima undangan dalam waktu tujuh hari, undangan tersebut akan kedaluwarsa secara otomatis.

Note

Beban kerja hanya dapat dibagi di dalam AWS Region yang sama.

Untuk menerima atau menolak undangan beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Undangan beban kerja.
3. Pilih undangan beban kerja yang akan diterima atau ditolak.
 - Pilih Terima untuk menerima undangan beban kerja.

Beban kerja ditambahkan ke halaman Beban Kerja dan Dasbor.

- Untuk menolak undangan beban kerja, pilih Tolak.

Undangan beban kerja akan dihapus dari daftar.

Untuk menolak akses bersama setelah undangan beban kerja diterima, pilih Tolak berbagi dari halaman [Melihat detail beban kerja di AWS Well-Architected Tool](#) untuk beban kerja.

Menghapus beban kerja di AWS Well-Architected Tool

Anda dapat menghapus beban kerja saat sudah tidak diperlukan. Menghapus beban kerja akan menghapus semua data yang terkait dengan beban kerja tersebut, termasuk titik pencapaian dan undangan berbagi beban kerja. Hanya pemilik yang dapat menghapus beban kerja.

Warning

Tindakan menghapus beban kerja tidak dapat diurungkan. Semua data yang terkait dengan beban kerja akan dihapus secara permanen.

Untuk menghapus beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang akan dihapus dan pilih Hapus.
4. Di jendela Hapus, pilih Hapus untuk mengonfirmasi penghapusan beban kerja dan titik pencapaiannya.

Agar suatu entitas tidak menghapus beban kerja, lampirkan kebijakan yang menyangkal tindakan `wellarchitected:DeleteWorkload`.

Menghasilkan laporan beban kerja di AWS Well-Architected Tool

Anda dapat menghasilkan laporan beban kerja untuk lensa. Laporan ini berisi respons Anda terhadap pertanyaan beban kerja, catatan Anda, dan jumlah risiko tinggi dan sedang yang teridentifikasi. Jika sebuah pertanyaan memiliki satu atau lebih risiko yang teridentifikasi, rencana perbaikan untuk pertanyaan tersebut akan mencantumkan tindakan yang harus diambil untuk menangani risiko tersebut.

Jika beban kerja Anda memiliki profil terkait, informasi ikhtisar profil dan risiko yang diprioritaskan akan ditampilkan di laporan beban kerja.

Laporan memungkinkan Anda untuk membagikan detail tentang beban kerja Anda kepada orang lain yang tidak memiliki akses ke AWS Well-Architected Tool.

Untuk menghasilkan laporan beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang diinginkan dan pilih Lihat detail.
4. Pilih lensa yang ingin Anda buat laporan, lalu pilih Hasilkan laporan.

Laporan akan dihasilkan dan Anda dapat mengunduh atau melihatnya.

Melihat detail beban kerja di AWS Well-Architected Tool

Halaman detail beban kerja memberikan informasi tentang beban kerja Anda termasuk titik pencapaian, rencana perbaikan, dan pembagian beban kerja apa pun. Gunakan tab di bagian atas halaman untuk membuka bagian detail lainnya.

Untuk menghapus beban kerja, pilih Hapus beban kerja. Hanya pemilik yang dapat menghapus beban kerja.

Untuk menghapus akses ke beban kerja bersama, pilih Tolak berbagi.

Topik

- [Tab Ikhtisar AWS Well-Architected Tool](#)
- [Tab Titik Pencapaian AWS Well-Architected Tool](#)
- [Tab Properti AWS Well-Architected Tool](#)
- [Tab Berbagi AWS Well-Architected Tool](#)

Tab Ikhtisar AWS Well-Architected Tool

Saat Anda pertama kali melihat beban kerja, tab Ikhtisar adalah informasi pertama yang ditampilkan. Tab ini menyediakan status keseluruhan beban kerja Anda diikuti dengan status masing-masing lensa.

Jika Anda belum menyelesaikan semua pertanyaan, banner akan muncul untuk mengingatkan Anda untuk memulai atau melanjutkan dokumentasi beban kerja.

Bagian Ikhtisar beban kerja menampilkan status keseluruhan beban kerja saat ini dan Catatan beban kerja apa pun yang telah Anda masukkan. Pilih Edit untuk memperbarui status atau catatan.

Untuk merekam status beban kerja saat ini, pilih Simpan titik pencapaian. Titik pencapaian bersifat tetap dan tidak dapat diubah setelah disimpan.

Untuk melanjutkan dokumentasi status beban kerja, pilih Mulai meninjau, lalu pilih lensa yang diinginkan.

Tab Titik Pencapaian AWS Well-Architected Tool

Untuk menampilkan titik pencapaian untuk beban kerja Anda, pilih tab Titik pencapaian.

Setelah Anda memilih titik pencapaian, pilih Hasilkan laporan untuk membuat laporan beban kerja yang terkait dengan titik pencapaian tersebut. Laporan tersebut berisi respons terhadap pertanyaan beban kerja, catatan Anda, dan jumlah risiko tinggi dan sedang dalam beban kerja pada saat titik pencapaian disimpan.

Anda dapat melihat detail tentang status beban kerja Anda pada saat titik pencapaian tertentu dengan:

- Memilih nama titik pencapaian.
- Memilih titik pencapaian dan memilih Lihat titik pencapaian.

Tab Properti AWS Well-Architected Tool

Untuk menampilkan properti beban kerja Anda, pilih tab Properti. Awalnya, properti ini adalah nilai yang ditentukan pada saat beban kerja ditetapkan. Pilih Edit untuk melakukan perubahan. Hanya pemilik beban kerja yang dapat melakukan perubahan.

Untuk deskripsi properti, lihat [Menentukan beban kerja di AWS WA Tool](#).

Tab Berbagi AWS Well-Architected Tool

Untuk menampilkan atau mengubah undangan beban kerja Anda, pilih tab Berbagi. Tab ini hanya ditampilkan untuk pemilik beban kerja.

Informasi berikut ini ditampilkan untuk setiap Akun AWS dan pengguna yang telah berbagi akses ke beban kerja:

Principal

ID Akun AWS atau ARN pengguna dengan akses bersama ke beban kerja.

Status

Status undangan beban kerja.

- Tertunda

Undangan sedang menunggu untuk diterima atau ditolak. Jika undangan beban kerja tidak diterima dalam waktu tujuh hari, undangan tersebut akan kedaluwarsa secara otomatis.

- Diterima

Undangan telah diterima.

- Ditolak

Undangan telah ditolak.

- Kedaluwarsa

Undangan tidak diterima atau ditolak dalam waktu tujuh hari.

Izin

Izin yang diberikan kepada Akun AWS atau pengguna.

- Hanya Baca

Principal memiliki akses hanya-baca ke beban kerja.

- Kontributor

Principal dapat memperbarui jawaban dan catatannya, dan memiliki akses hanya-baca ke sisa beban kerja.

Detail izin

Detail deskripsi tentang izin.

Untuk berbagi beban kerja dengan Akun AWS atau pengguna lain di AWS Region yang sama, pilih Buat. Beban kerja dapat dibagikan dengan hingga 20 Akun AWS dan pengguna berbeda.

Untuk menghapus undangan beban kerja, pilih undangan dan pilih Hapus.

Untuk mengubah undangan beban kerja, pilih undangan dan pilih Edit.

Menggunakan lensa di AWS WA Tool

Di AWS Well-Architected Tool, Anda dapat menggunakan lensa untuk secara konsisten mengukur arsitektur Anda berdasarkan praktik terbaik dan mengidentifikasi area yang perlu ditingkatkan. Lensa Kerangka Kerja AWS Well-Architected secara otomatis diterapkan ketika beban kerja ditentukan.

Beban kerja dapat memiliki satu atau beberapa lensa yang diterapkan. Setiap lensa memiliki serangkaian pertanyaan, praktik terbaik, catatan, dan rencana perbaikannya sendiri.

Ada dua jenis lensa yang dapat diterapkan pada beban kerja Anda: Lensa dari Katalog Lensa dan lensa kustom.

- [Katalog Lensa](#): Lensa resmi yang dibuat dan dipelihara oleh AWS. Katalog Lensa tersedia untuk semua pengguna dan tidak memerlukan penginstalan tambahan untuk digunakan.
- [Lensa kustom](#): Lensa yang ditentukan pengguna yang bukan konten resmi AWS. Anda dapat [membuat lensa kustom](#) dengan pilar, pertanyaan, praktik terbaik, dan rencana perbaikan Anda sendiri, serta [membagikan lensa kustom](#) ke Akun AWS lain.

Lima lensa dapat ditambahkan sekaligus ke beban kerja, dengan maksimal 20 lensa diterapkan pada satu beban kerja.

Jika lensa dihapus dari beban kerja, data yang terkait dengan lensa dipertahankan. Data dipulihkan jika Anda menambahkan lensa kembali ke beban kerja.

Menambahkan lensa ke beban kerja di AWS WA Tool

Menambahkan lensa ke beban kerja membantu Anda lebih memahami kekuatan dan kelemahan arsitektur Anda, mengidentifikasi peningkatan yang diperlukan, dan memastikan beban kerja Anda mengikuti praktik terbaik.

Untuk menambahkan lensa ke beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang diinginkan dan pilih Lihat detail.
4. Pilih lensa yang akan ditambahkan dan pilih Simpan.

Lensa dapat dipilih dari Lensa kustom, Katalog Lensa, atau keduanya.

Hingga 20 lensa dapat ditambahkan ke beban kerja.

Untuk informasi lebih lanjut tentang katalog lensa AWS, kunjungi [Lensa AWS Well-Architected](#). Perhatikan bahwa tidak setiap laporan resmi lensa disediakan sebagai lensa dalam katalog lensa.

Sanggahan

Dengan mengakses dan/atau menerapkan lensa kustom yang dibuat oleh pengguna atau akun AWS lain, Anda memahami bahwa lensa kustom yang dibuat oleh pengguna lain dan dibagikan kepada Anda adalah Konten Pihak Ketiga sebagaimana didefinisikan dalam Perjanjian Pelanggan AWS.

Menghapus lensa dari beban kerja di AWS WA Tool

Jika lensa tidak lagi relevan dengan beban kerja Anda, Anda dapat menghapusnya.

Untuk menghapus lensa dari beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang diinginkan dan pilih Lihat detail.
4. Hapus pilihan lensa yang ingin dihapus dan pilih Simpan.

Lensa AWS Kerangka Well-Architected tidak dapat dihapus dari beban kerja.

Data yang terkait dengan lensa dipertahankan. Jika lensa ditambahkan kembali ke beban kerja, data dipulihkan.

Melihat detail lensa untuk beban kerja di AWS WA Tool

Anda dapat melihat detail tentang lensa di konsol AWS Well-Architected Tool. Untuk melihat detail tentang lensa, pilih lensa.

Tab Gambaran umum

Tab Gambaran umum memberikan informasi umum tentang lensa, seperti jumlah pertanyaan yang dijawab. Dari tab ini, Anda dapat melanjutkan meninjau beban kerja, membuat laporan, atau mengedit catatan lensa.

Tab Rencana perbaikan

Tab Rencana perbaikan menyediakan daftar tindakan yang disarankan untuk meningkatkan beban kerja Anda. Anda dapat memfilter rekomendasi berdasarkan risiko dan pilar.

Tab Berbagi

Untuk lensa kustom, tab Berbagi menyediakan daftar principal IAM yang telah menerima pembagian lensa.

Lensa kustom untuk beban kerja di AWS WA Tool

Anda dapat membuat lensa kustom dengan pilar, pertanyaan, praktik terbaik, dan rencana perbaikan Anda sendiri. Anda menerapkan lensa kustom ke beban kerja dengan cara yang sama seperti Anda menerapkan lensa yang disediakan AWS. Anda juga dapat membagikan lensa kustom yang Anda buat ke Akun AWS lain, dan lensa kustom yang dimiliki oleh orang lain dapat dibagikan kepada Anda.

Anda dapat menyesuaikan pertanyaan dalam lensa kustom agar spesifik untuk teknologi tertentu, membantu Anda memenuhi kebutuhan tata kelola dalam organisasi Anda, atau memperluas panduan yang diberikan oleh Kerangka Kerja Well-Architected dan lensa AWS. Seperti lensa yang ada, Anda dapat melacak progres dari waktu ke waktu dengan membuat tonggak pencapaian, dan memberikan status berkala dengan menghasilkan laporan.

Topik

- [Melihat lensa kustom di AWS WA Tool](#)
- [Membuat lensa kustom untuk beban kerja di AWS WA Tool](#)
- [Melihat pratinjau lensa kustom untuk beban kerja di AWS WA Tool](#)
- [Memublikasikan lensa kustom AWS WA Tool untuk pertama kalinya](#)
- [Memublikasikan pembaruan ke lensa kustom di AWS WA Tool](#)
- [Membagikan lensa kustom di AWS WA Tool](#)

- [Menambahkan tanda ke lensa kustom di AWS WA Tool](#)
- [Menghapus lensa kustom di AWS WA Tool](#)
- [Spesifikasi format lensa di AWS WA Tool](#)

Melihat lensa kustom di AWS WA Tool

Anda dapat melihat detail lensa kustom yang Anda miliki dan lensa kustom yang telah dibagikan kepada Anda.

Untuk melihat lensa

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Lensa kustom.

Note

Bagian Lensa kustom kosong jika Anda belum membuat lensa kustom atau memiliki lensa kustom yang dibagikan kepada Anda.

3. Pilih lensa kustom yang ingin Anda lihat:
 - Dimiliki oleh saya – Menampilkan lensa kustom yang telah Anda buat.
 - Berbagi dengan saya – Menampilkan lensa kustom yang telah dibagikan kepada Anda.
4. Pilih lensa kustom untuk dilihat dengan salah satu cara berikut:
 - Pilih nama lensa.
 - Pilih lensa dan pilih Lihat detail.

Halaman [Melihat detail lensa untuk beban kerja di AWS WA Tool](#) ditampilkan.

Halaman Lensa kustom memiliki bidang-bidang berikut:

Nama

Nama lensa.

Pemilik

ID Akun AWS yang merupakan pemilik lensa kustom.

Status

Status DIPUBLIKASIKAN berarti bahwa lensa kustom telah dipublikasikan dan dapat diterapkan pada beban kerja atau dibagikan ke Akun AWS lain.

Status DRAF berarti bahwa lensa kustom telah dibuat, tetapi belum dipublikasikan. Lensa kustom harus dipublikasikan sebelum dapat diterapkan pada beban kerja atau dibagikan.

Versi

Nama versi lensa kustom.

Terakhir diperbarui

Tanggal dan waktu lensa kustom terakhir diperbarui.

Membuat lensa kustom untuk beban kerja di AWS WA Tool

Untuk membuat lensa kustom

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih Buat lensa kustom.
4. Pilih Unduh file untuk mengunduh file templat JSON.
5. Buka file templat JSON dengan editor teks favorit Anda dan tambahkan data untuk lensa kustom Anda. Data ini mencakup pilar, pertanyaan, praktik terbaik, dan tautan rencana perbaikan Anda.

Lihat [Spesifikasi format lensa di AWS WA Tool](#) untuk detailnya. Lensa kustom tidak boleh melebihi 500 KB.

6. Gunakan Pilih file untuk memilih file JSON Anda.
7. (Opsional) Di bagian Tanda, tambahkan tanda yang ingin Anda kaitkan dengan beban kerja.
8. Pilih Kirim & Pratinjau untuk melihat pratinjau lensa kustom, atau Kirim untuk mengirimkan lensa kustom tanpa melihat pratinjau.

Jika Anda memilih Kirim & Pratinjau untuk lensa kustom Anda, Anda dapat memilih Berikutnya untuk menavigasi melalui pratinjau lensa, atau pilih Keluar dari Pratinjau untuk kembali ke Lensa kustom.

Jika validasi gagal, edit file JSON Anda dan coba buat lensa kustom lagi.

Setelah AWS WA Tool memvalidasi file JSON Anda, lensa kustom Anda ditampilkan di Lensa kustom.

Setelah lensa kustom dibuat, statusnya menjadi DRAF. Anda harus [memublikasikan lensa](#) sebelum dapat diterapkan ke beban kerja atau dibagikan ke Akun AWS lain.

Anda dapat membuat hingga 15 lensa kustom di Akun AWS.

Sanggahan

Jangan menyertakan atau mengumpulkan informasi pengenal pribadi (PII) pengguna akhir atau individu lain yang dapat diidentifikasi di dalam atau melalui lensa kustom Anda. Jika lensa kustom Anda atau yang dibagikan kepada Anda dan digunakan di akun Anda menyertakan atau mengumpulkan PII, Anda bertanggung jawab untuk: memastikan bahwa PII yang disertakan diproses sesuai dengan hukum yang berlaku, memberikan pemberitahuan privasi yang memadai, dan mendapatkan persetujuan yang diperlukan untuk memproses data tersebut.

Melihat pratinjau lensa kustom untuk beban kerja di AWS WA Tool

Untuk melihat pratinjau lensa kustom

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Hanya lensa dalam status DRAF yang dapat dilihat pratinjaunya. Pilih lensa kustom DRAF yang diinginkan dan pilih Pratinjau pengalaman.
4. Pilih Berikutnya untuk menavigasi melalui pratinjau lensa.
5. (Opsional) Anda dapat meninjau Rencana perbaikan Anda dengan memilih praktik terbaik dalam setiap pertanyaan di pratinjau, dan memilih Perbarui berdasarkan jawaban untuk menguji logika risiko Anda. Jika ada perubahan yang diperlukan, Anda dapat memperbarui [Aturan Risiko](#) di templat JSON Anda sebelum memublikasikan.
6. Pilih Keluar dari Pratinjau untuk kembali ke lensa kustom.

Note

Anda juga dapat melihat pratinjau lensa kustom dengan memilih Kirim & Pratinjau saat [Membuat lensa kustom](#).

Memublikasikan lensa kustom AWS WA Tool untuk pertama kalinya

Untuk memublikasikan lensa kustom

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa kustom yang diinginkan dan pilih Publikasikan lensa.
4. Di kotak Nama versi, masukkan pengidentifikasi unik untuk perubahan versi. Nilai ini bisa memiliki 32 karakter dan hanya boleh berisi karakter alfanumerik dan titik (".").
5. Pilih Publikasikan lensa kustom.

Setelah lensa kustom dipublikasikan, statusnya menjadi DIPUBLIKASIKAN.

Lensa kustom sekarang dapat diterapkan ke beban kerja atau dibagikan ke Akun AWS atau pengguna lain.

Memublikasikan pembaruan ke lensa kustom di AWS WA Tool

Untuk memublikasikan pembaruan ke lensa kustom yang ada

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa kustom yang diinginkan dan pilih Edit.
4. Jika Anda belum memiliki file JSON yang diperbarui, pilih Unduh file untuk mengunduh salinan lensa kustom saat ini. Edit file JSON yang diunduh dengan editor teks favorit Anda dan buat perubahan yang Anda inginkan.

5. Gunakan Pilih file untuk memilih file JSON yang diperbarui dan pilih Kirim & Pratinjau untuk melihat pratinjau lensa kustom, atau Kirim untuk mengirimkan lensa kustom tanpa melihat pratinjau.

Lensa kustom tidak boleh melebihi 500 KB.

Setelah AWS WA Tool memvalidasi file JSON Anda, lensa kustom Anda ditampilkan di Lensa kustom dalam status DRAF.

6. Pilih lensa kustom lagi dan pilih Publikasikan lensa.
7. Pilih Tinjau perubahan sebelum memublikasikan untuk memeriksa bahwa perubahan yang dilakukan pada lensa kustom Anda sudah benar. Tindakan ini termasuk memvalidasi:
 - Nama lensa kustom.
 - Nama pilar
 - Pertanyaan baru, diperbarui, dan dihapus

Pilih Berikutnya.

8. Tentukan jenis perubahan versi.

Versi utama

Menunjukkan bahwa perubahan besar telah dilakukan pada lensa. Gunakan untuk perubahan yang memengaruhi arti lensa kustom.

Beban kerja yang menerapkan lensa akan mendapatkan notifikasi bahwa lensa kustom versi baru tersedia.

Perubahan versi utama tidak diterapkan secara otomatis ke beban kerja yang menggunakan lensa.

Versi minor

Menunjukkan bahwa perubahan kecil telah dilakukan pada lensa. Gunakan untuk perubahan kecil, seperti perubahan teks atau pembaruan tautan URL.

Perubahan versi minor secara otomatis diterapkan ke beban kerja menggunakan lensa kustom.

Pilih Berikutnya.

9. Di kotak Nama versi, masukkan pengidentifikasi unik untuk perubahan versi. Nilai ini bisa memiliki 32 karakter dan hanya boleh berisi karakter alfanumerik dan titik (".").
10. Pilih Publikasikan lensa kustom.

Setelah lensa kustom dipublikasikan, statusnya menjadi DIPUBLIKASIKAN.

Lensa kustom yang diperbarui sekarang dapat diterapkan ke beban kerja atau dibagikan ke Akun AWS atau pengguna lain.

Jika pembaruannya adalah perubahan versi utama, beban kerja apa pun yang menerapkan versi lensa sebelumnya akan mendapatkan notifikasi bahwa versi baru tersedia dan diberi opsi untuk peningkatan.

Pembaruan versi minor diterapkan secara otomatis tanpa notifikasi apa pun.

Anda dapat membuat hingga 100 versi lensa kustom.

Membagikan lensa kustom di AWS WA Tool

Anda dapat membagikan lensa kustom ke Akun AWS, pengguna, AWS Organizations, dan unit organisasi (OU) lain.

Untuk membagikan lensa kustom ke Akun AWS dan pengguna lain

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa kustom yang akan dibagikan dan pilih Lihat detail.
4. Pada halaman [Melihat detail lensa untuk beban kerja di AWS WA Tool](#), pilih Berbagi. Kemudian pilih Buat dan Buat pembagian ke pengguna atau akun untuk membuat undangan berbagi lensa.
5. Masukkan ID Akun AWS 12 digit atau ARN pengguna yang ingin Anda bagi lensa kustom.
6. Pilih Buat untuk mengirim undangan berbagi lensa ke Akun AWS atau pengguna yang ditentukan.

Anda dapat membagikan lensa kustom ke maksimal 300 Akun AWS atau pengguna.

Jika undangan berbagi lensa tidak disetujui dalam waktu tujuh hari, undangan tersebut akan kedaluwarsa secara otomatis.

⚠ Important

Sebelum membagikan lensa kustom ke organisasi atau unit organisasi (OU), Anda harus [mengaktifkan akses AWS Organizations](#).

Untuk membagikan lensa kustom ke organisasi atau OU

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa kustom yang akan dibagikan.
4. Pada halaman [Melihat detail lensa untuk beban kerja di AWS WA Tool](#), pilih Berbagi. Kemudian pilih Buat dan Buat pembagian ke Organisasi.
5. Pada halaman Buat berbagi lensa kustom, pilih apakah akan memberikan izin ke seluruh organisasi, atau ke satu atau beberapa OU.
6. Pilih Buat untuk membagikan lensa kustom.

Untuk melihat siapa yang memiliki akses ke lensa kustom yang dibagikan, pilih Berbagi dari halaman [Melihat detail lensa untuk beban kerja di AWS WA Tool](#).

ℹ Sanggahan

Dengan membagikan lensa kustom Anda ke Akun AWS lain, Anda memahami bahwa AWS akan membuat lensa kustom Anda tersedia untuk akun lain tersebut. Akun lain tersebut dapat terus mengakses dan menggunakan lensa kustom yang dibagikan meskipun Anda menghapus lensa kustom tersebut dari Akun AWS Anda sendiri atau menghentikan Akun AWS Anda.

Menambahkan tanda ke lensa kustom di AWS WA Tool

Untuk menambahkan tanda ke lensa kustom

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.

2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa kustom yang ingin Anda perbarui.
4. Di bagian Tanda, pilih Kelola tanda.
5. Pilih Tambahkan tanda baru lalu masukkan Kunci dan Nilai untuk setiap tanda yang ingin Anda tambahkan.
6. Pilih Simpan.

Untuk menghapus tanda, pilih Hapus di samping tanda yang ingin dihapus.

Menghapus lensa kustom di AWS WA Tool

Untuk menghapus lensa kustom

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa kustom yang akan dihapus dan pilih Hapus.
4. Pilih Hapus.

Beban kerja yang ada yang menerapkan lensa akan menerima notifikasi bahwa lensa kustom telah dihapus, tetapi dapat terus menggunakannya. Lensa kustom tidak dapat lagi diterapkan pada beban kerja baru.

Sanggahan

Dengan membagikan lensa kustom Anda ke Akun AWS lain, Anda memahami bahwa AWS akan membuat lensa kustom Anda tersedia untuk akun lain tersebut. Akun lain tersebut dapat terus mengakses dan menggunakan lensa kustom yang dibagikan meskipun Anda menghapus lensa kustom tersebut dari Akun AWS Anda sendiri atau menghentikan Akun AWS Anda.

Spesifikasi format lensa di AWS WA Tool

Lensa didefinisikan menggunakan format JSON tertentu. Saat Anda mulai membuat lensa kustom, Anda memiliki opsi untuk mengunduh file JSON templat. Anda dapat menggunakan file ini sebagai

dasar untuk lensa kustom Anda karena mendefinisikan struktur dasar untuk pilar, pertanyaan, praktik terbaik, dan rencana perbaikan.

Bagian Lensa

Bagian ini mendefinisikan atribut untuk lensa kustom itu sendiri. Ini adalah nama dan deskripsinya.

- `schemaVersion`: Versi skema lensa kustom yang akan digunakan. Ditetapkan oleh templat, tidak akan berubah.
- `name`: Nama lensa. Nama dapat memiliki maksimal 128 karakter.
- `description`: Deskripsi teks untuk lensa. Teks ini ditampilkan saat memilih lensa yang akan ditambahkan selama pembuatan beban kerja, atau saat memilih lensa yang akan diterapkan pada beban kerja yang ada nanti. Deskripsi dapat memiliki maksimal 2048 karakter.

```
"schemaVersion": "2021-11-01",  
"name": "Company Policy ABC",  
"description": "This lens provides a set of specific questions to assess compliance  
with company policy ABC-2021 as revised on 2021/09/01.",
```

Bagian Pilar

Bagian ini mendefinisikan pilar yang terkait dengan lensa kustom. Anda dapat memetakan pertanyaan Anda ke pilar Kerangka Kerja AWS Well-Architected, menentukan pilar Anda sendiri, atau keduanya.

Anda dapat menentukan hingga 10 pilar dalam lensa kustom.

- `id`: ID untuk pilar. ID ini dapat memiliki antara 3 dan 128 karakter dan hanya berisi karakter alfanumerik dan garis bawah ("_"). ID yang digunakan dalam pilar harus unik.

Saat memetakan pertanyaan Anda ke pilar Kerangka Kerja, gunakan ID berikut:

- `operationalExcellence`
- `security`
- `reliability`
- `performance`
- `costOptimization`

- `sustainability`
- `name`: Nama pilar. Nama dapat memiliki maksimal 128 karakter.

```
"pillars": [  
  {  
    "id": "company_Privacy",  
    "name": "Privacy Excellence",  
    .  
    .  
    .  
  },  
  {  
    "id": "company_Security",  
    "name": "Security",  
    .  
    .  
    .  
  }  
]
```

Bagian Pertanyaan

Bagian ini mendefinisikan pertanyaan yang terkait dengan pilar.

Anda dapat menentukan hingga 20 pertanyaan dalam sebuah pilar di lensa kustom.

- `id`: ID untuk pertanyaan. ID dapat memiliki 3 hingga 128 karakter dan hanya berisi karakter alfanumerik dan garis bawah ("_"). ID yang digunakan dalam pertanyaan harus unik.
- `title`: Judul pertanyaan. Nama dapat memiliki maksimal 128 karakter.
- `description`: Menjelaskan pertanyaan secara lebih mendetail. Deskripsi dapat memiliki maksimal 2048 karakter.
- `helpfulResource displayText`: Opsional. Teks yang memberikan informasi bermanfaat tentang pertanyaan. Teks dapat memiliki maksimal 2048 karakter. Harus ditentukan jika `helpfulResource url` ditentukan.
- `helpfulResource url`: Opsional. Sumber daya URL yang menjelaskan pertanyaan secara lebih mendetail. URL harus dimulai dengan `http://` atau `https://`.

Note

Saat menyinkronkan beban kerja lensa kustom ke Jira, pertanyaan menampilkan "id" dan "judul" pertanyaan.

Format yang digunakan dalam tiket Jira adalah [QuestionID] QuestionTitle.

```
"questions": [  
  {  
    "id": "privacy01",  
    "title": "How do you ensure HR conversations are private?",  
    "description": "Career and benefits discussions should occur on secure channels only and be audited regularly for compliance.",  
    "helpfulResource": {  
      "displayText": "This is helpful text for the first question",  
      "url": "https://example.com/poptquest01_help.html"  
    },  
    .  
    .  
    .  
  },  
  {  
    "id": "privacy02",  
    "title": "Is your team following the company privacy policy?",  
    "description": "Our company requires customers to opt-in to data use and does not disclose customer data to third parties either individually or in aggregate.",  
    "helpfulResource": {  
      "displayText": "This is helpful text for the second question",  
      "url": "https://example.com/poptquest02_help.html"  
    },  
    .  
    .  
    .  
  }  
]
```

Bagian Pilihan

Bagian ini mendefinisikan pilihan yang terkait dengan pertanyaan.

Anda dapat menentukan hingga 15 pilihan untuk pertanyaan dalam lensa kustom.

- `id`: ID untuk pilihan. ID ini dapat memiliki antara 3 dan 128 karakter dan hanya berisi karakter alfanumerik dan garis bawah ("_"). ID unik harus ditentukan untuk setiap pilihan dalam pertanyaan. Menambahkan pilihan dengan akhiran `_no` akan berfungsi sebagai pilihan `None of these` untuk pertanyaan.
- `title`: Judul pilihan. Nama dapat memiliki maksimal 128 karakter.
- `helpfulResource displayText`: Opsional. Teks yang memberikan informasi bermanfaat tentang pilihan. Teks dapat memiliki maksimal 2048 karakter. Harus disertakan jika `helpfulResource url` ditentukan.
- `helpfulResource url`: Opsional. Sumber daya URL yang menjelaskan pilihan secara lebih mendetail. URL harus dimulai dengan `http://` atau `https://`.
- `improvementPlan displayText`: Teks yang menjelaskan bagaimana pilihan dapat ditingkatkan. Teks dapat memiliki maksimal 2048 karakter. `improvementPlan` diperlukan untuk setiap pilihan, kecuali untuk pilihan `None of these`.
- `improvementPlan url`: Opsional. Sumber daya URL yang dapat membantu peningkatan. URL harus dimulai dengan `http://` atau `https://`.
- `additionalResources type`: Opsional. Jenis sumber daya tambahan. Nilai dapat berupa `HELPFUL_RESOURCE` atau `IMPROVEMENT_PLAN`.
- `additionalResources content`: Opsional. Menentukan nilai `displayText` dan `url` untuk sumber daya tambahan. Hingga lima sumber daya yang berguna tambahan dan hingga lima item rencana perbaikan tambahan dapat ditentukan untuk sebuah pilihan.
 - `displayText`: Opsional. Teks yang menjelaskan sumber daya yang berguna atau rencana perbaikan. Teks dapat memiliki maksimal 2048 karakter. Harus disertakan jika `url` ditentukan.
 - `url`: Opsional. Sumber daya URL untuk sumber daya yang berguna atau rencana perbaikan. URL harus dimulai dengan `http://` atau `https://`.

Note

Saat menyinkronkan beban kerja lensa kustom ke Jira, pilihan menampilkan "id" pertanyaan dan pilihan, serta "judul" pilihan.

Format yang digunakan adalah `[QuestionID | ChoiceID] ChoiceTitle`.

```
"choices": [
  {
```

```

    "id": "choice_1",
    "title": "Option 1",
    "helpfulResource": {
      "displayText": "This is helpful text for the first choice",
      "url": "https://example.com/popt01_help.html"
    },
    "improvementPlan": {
      "displayText": "This is text that will be shown for improvement of
this choice.",
      "url": "https://example.com/popt01_iplan.html"
    }
  },
  {
    "id": "choice_2",
    "title": "Option 2",
    "helpfulResource": {
      "displayText": "This is helpful text for the second choice",
      "url": "https://example.com/hr_manual_CORP_1.pdf"
    },
    "improvementPlan": {
      "displayText": "This is text that will be shown for improvement of
this choice.",
      "url": "https://example.com/popt02_iplan_01.html"
    },
    "additionalResources": [
      {
        "type": "HELPFUL_RESOURCE",
        "content": [
          {
            "displayText": "This is the second set of helpful text for this
choice.",
            "url": "https://example.com/hr_manual_country.html"
          },
          {
            "displayText": "This is the third set of helpful text for this
choice.",
            "url": "https://example.com/hr_manual_city.html"
          }
        ]
      }
    ],
    "type": "IMPROVEMENT_PLAN",
    "content": [
      {

```

```

        "displayText": "This is additional text that will be shown for
improvement of this choice.",
        "url": "https://example.com/popt02_ipplan_02.html"
    },
    {
        "displayText": "This is the third piece of improvement plan
text.",
        "url": "https://example.com/popt02_ipplan_03.html"
    }
    {
        "displayText": "This is the fourth piece of improvement plan
text.",
        "url": "https://example.com/popt02_ipplan_04.html"
    }
    ]
}
],
{
    "id": "option_no",
    "title": "None of these",
    "helpfulResource": {
        "displayText": "Choose this if your workload does not follow these best
practices.",
        "url": "https://example.com/popt02_ipplan_none.html"
    }
}
}

```

Bagian Aturan Risiko

Bagian ini mendefinisikan bagaimana pilihan yang dipilih menentukan tingkat risiko.

Anda dapat menentukan maksimal tiga aturan risiko per pertanyaan, satu untuk setiap tingkat risiko.

- **condition**: Ekspresi Boolean dari pilihan yang dipetakan ke tingkat risiko untuk pertanyaan, atau default.

Harus ada aturan risiko default untuk setiap pertanyaan.

- **risk**: Menunjukkan risiko yang terkait dengan kondisi. Nilai yang valid adalah HIGH_RISK, MEDIUM_RISK, dan NO_RISK.

Urutan aturan risiko Anda penting. `condition` pertama yang dievaluasi menjadi `true` menetapkan risiko untuk pertanyaan. Pola umum untuk menerapkan aturan risiko adalah memulai dengan aturan yang paling tidak berisiko (dan biasanya paling terperinci) dan melanjutkan ke aturan Anda yang paling berisiko (dan paling tidak spesifik).

Misalnya:

```
"riskRules": [  
  {  
    "condition": "choice_1 && choice_2 && choice_3",  
    "risk": "NO_RISK"  
  },  
  {  
    "condition": "((choice_1 || choice_2) && choice_3) || (!choice_1 && choice_3)",  
    "risk": "MEDIUM_RISK"  
  },  
  {  
    "condition": "default",  
    "risk": "HIGH_RISK"  
  }  
]
```

Jika pertanyaan memiliki tiga pilihan (`choice_1`, `choice_2`, dan `choice_3`), aturan risiko ini menghasilkan perilaku berikut:

- Jika ketiga pilihan digunakan, tidak ada risiko.
- Jika `choice_1` atau `choice_2` dipilih dan `choice_3` dipilih, ada risiko sedang.
- Jika `choice_1` tidak dipilih tetapi `choice_3` dipilih, ada juga risiko sedang.
- Jika tidak satu pun dari kondisi sebelumnya benar, ada risiko tinggi.

Peningkatan lensa di AWS WA Tool

Lensa Kerangka Kerja AWS Well-Architected dan lensa lain yang disediakan oleh AWS diperbarui seiring layanan-layanan baru diperkenalkan, praktik terbaik yang ada untuk sistem berbasis cloud disempurnakan, dan praktik terbaik baru ditambahkan. Saat lensa versi baru tersedia, AWS WA Tool akan ditingkatkan untuk mencerminkan praktik terbaik terbaru. Beban kerja baru yang ditentukan akan menggunakan lensa versi baru.

Peningkatan lensa juga terjadi ketika lensa kustom yang telah Anda terapkan pada beban kerja atau templat tinjauan memiliki versi utama baru yang dipublikasikan.

Peningkatan lensa dapat terdiri dari kombinasi:

- Menambahkan pertanyaan atau praktik terbaik baru
- Menghapus pertanyaan atau praktik lama yang tidak lagi direkomendasikan
- Memperbarui pertanyaan atau praktik terbaik yang ada
- Menambahkan atau menghapus pilar

Jawaban Anda atas pertanyaan yang ada akan dipertahankan.

Note

Anda tidak dapat membatalkan peningkatan lensa. Setelah beban kerja ditingkatkan ke versi lensa terbaru, Anda tidak dapat kembali ke versi lensa sebelumnya.

Menentukan lensa mana yang akan ditingkatkan di AWS WA Tool

Anda dapat menemukan beban kerja mana yang tidak menggunakan versi lensa terbaru dengan melihat halaman Notifikasi.

Informasi berikut ditampilkan di halaman Notifikasi untuk setiap beban kerja:

Sumber Daya

Nama beban kerja atau templat tinjauan.

Jenis sumber daya

Jenis sumber daya. Ini bisa berupa Beban kerja atau Templat tinjauan.

Sumber daya terkait

Nama lensa.

Jenis notifikasi

Jenis notifikasi peningkatan.

- Tidak saat ini – Beban kerja menggunakan versi lensa yang tidak lagi terkini. Tingkatkan ke versi lensa saat ini untuk panduan yang lebih baik.

- Usang – Beban kerja menggunakan versi lensa yang tidak lagi mencerminkan praktik terbaik. Tingkatkan ke versi lensa saat ini.
- Dihapus – Beban kerja menggunakan lensa yang telah dihapus oleh pemiliknya.

Versi yang digunakan

Versi lensa saat ini digunakan untuk beban kerja.

Versi yang tersedia saat ini

Versi lensa yang tersedia untuk peningkatan, atau Tidak ada jika lensa telah dihapus.

Untuk meningkatkan lensa yang terkait dengan beban kerja, pilih beban kerja dan pilih Tingkatkan versi lensa.

Meningkatkan lensa di AWS WA Tool

Lensa dapat ditingkatkan untuk beban kerja dan templat tinjauan.

Note

Anda tidak dapat membatalkan peningkatan lensa. Setelah templat beban kerja atau tinjauan ditingkatkan ke versi lensa terbaru, Anda tidak dapat kembali ke versi lensa sebelumnya.

Meningkatkan lensa untuk beban kerja

1. Pada halaman Notifikasi, pilih beban kerja yang akan ditingkatkan, dan pilih Tingkatkan versi lensa. Informasi tentang apa yang berubah di setiap pilar akan ditampilkan.

Note

Anda juga dapat memilih Lihat peningkatan yang tersedia dari tab Gambaran umum beban kerja.

2. Sebelum meningkatkan lensa untuk beban kerja, tonggak pencapaian dibuat untuk menyimpan status beban kerja Anda yang ada untuk referensi mendatang. Masukkan nama unik untuk tonggak pencapaian di kolom Nama tonggak pencapaian.
3. Centang kotak Konfirmasi di sebelah Saya mengerti dan menerima perubahan ini dan pilih Simpan.

Setelah lensa ditingkatkan, Anda dapat melihat versi lensa sebelumnya dari tab Tonggak pencapaian.

Meningkatkan lensa untuk templat tinjauan

1. Guna meningkatkan lensa untuk templat tinjauan, pilih
2. Pada halaman Notifikasi, pilih templat tinjauan yang akan ditingkatkan, dan pilih Tingkatkan versi lensa. Informasi tentang apa yang berubah di setiap pilar akan ditampilkan.

Note

Anda juga dapat memilih Lihat peningkatan yang tersedia dari tab Gambaran umum templat tinjauan.

3. Centang kotak Konfirmasi di sebelah Saya mengerti dan menerima perubahan ini dan pilih Tingkatkan dan edit jawaban templat guna menyesuaikan jawaban atas pertanyaan praktik terbaik untuk templat tinjauan Anda, atau Tingkatkan guna meningkatkan lensa tanpa menyesuaikan jawaban templat Anda.

Katalog Lensa untuk AWS WA Tool

Katalog Lensa adalah kumpulan lensa AWS resmi yang dibuat untuk AWS Well-Architected Tool yang menawarkan teknologi dan praktik terbaik terkini yang berfokus pada industri. Lensa ini tersedia untuk semua pengguna dan tidak memerlukan penginstalan tambahan untuk digunakan.

Tabel berikut menjelaskan semua lensa resmi AWS yang saat ini tersedia di Katalog Lensa.

Nama file	Deskripsi
Kerangka Kerja AWS Well-Architected	Diterapkan secara default ke semua beban kerja. Kumpulan praktik terbaik arsitektur untuk mendesain dan mengoperasikan sistem yang andal, aman, efisien, hemat biaya, dan ramah lingkungan di cloud.
Mobilitas Terhubung	Praktik terbaik untuk mengintegrasikan teknologi ke dalam sistem transportasi dan

Nama file	Deskripsi
	meningkatkan pengalaman mobilitas secara keseluruhan.
Build Kontainer	Memberikan praktik terbaik terkait desain kontainer dan proses build.
Analitik Data	Berisi wawasan yang telah dikumpulkan AWS dari studi kasus dunia nyata, dan akan membantu Anda mempelajari elemen desain utama dari beban kerja analitik Well-Architected, bersama dengan rekomendasi untuk perbaikan.
DevOps	Menjelaskan pendekatan terstruktur yang dapat diikuti oleh organisasi dari semua ukuran untuk menumbuhkan budaya berkecepatan tinggi yang berfokus pada keamanan yang mampu memberikan nilai bisnis yang substansial menggunakan teknologi modern dan praktik terbaik DevOps.
Industri Jasa Keuangan	Praktik terbaik untuk merancang beban kerja Industri Jasa Keuangan Anda di AWS.
AI Generatif	Praktik terbaik untuk merancang beban kerja AI generatif Anda di AWS.
Pemerintah	Praktik terbaik untuk merancang dan memberikan layanan pemerintah di AWS.
Industri Perawatan Kesehatan	Praktik terbaik dan panduan tentang cara merancang, men-deploy, dan mengelola beban kerja perawatan kesehatan Anda di AWS Cloud.
IoT	Praktik terbaik untuk mengelola beban kerja Internet untuk Segala (IoT) Anda di AWS.

Nama file	Deskripsi
Merger dan Akuisisi	Praktik terbaik untuk integrasi dan migrasi beban kerja ke cloud selama merger dan akuisisi.
Machine Learning	Praktik terbaik untuk mengelola sumber daya dan beban kerja Machine Learning Anda di AWS.
Migrasi	Praktik terbaik tentang cara bermigrasi ke AWS Cloud.
SaaS	Berfokus untuk merancang, men-deploy, dan merancang beban kerja perangkat lunak sebagai layanan (SaaS) Anda di AWS Cloud.
SAP	Prinsip desain dan praktik terbaik untuk beban kerja SAP di AWS Cloud.
Aplikasi Nirserver	Praktik terbaik untuk membangun beban kerja nirserver di AWS. Meliputi skenario seperti layanan mikro RESTful, backend aplikasi seluler, pemrosesan stream, dan aplikasi web.

Tinjau template di AWS WA Tool

Anda dapat membuat template ulasan AWS WA Tool yang berisi jawaban yang telah diisi sebelumnya untuk Well-Architected Framework dan pertanyaan praktik terbaik lensa kustom. Templat tinjauan Well-Architected mengurangi kebutuhan untuk secara manual mengisi jawaban yang sama untuk praktik terbaik yang umum di beberapa beban kerja saat melakukan tinjauan Well-Architected, dan membantu mendorong konsistensi dan standarisasi praktik terbaik di seluruh tim dan beban kerja.

Anda dapat [membuat templat ulasan](#) untuk menjawab pertanyaan praktik terbaik umum atau membuat catatan, yang dapat dibagikan dengan IAM pengguna atau akun lain, atau organisasi atau unit organisasi yang sama AWS Region. Anda dapat [menentukan beban kerja dari templat ulasan](#), yang membantu menskalakan praktik terbaik umum dan mengurangi redundansi di seluruh beban kerja Anda.

Membuat template ulasan di AWS WA Tool


Untuk membuat template ulasan

1. Pilih Tinjau templat di panel navigasi kiri.
2. Pilih Buat templat.
3. Pada halaman Tentukan detail templat, berikan Nama dan Deskripsi untuk templat ulasan Anda.
4. (Opsional) Di catatan Template dan Tag bagian, tambahkan catatan template atau tag yang ingin Anda kaitkan dengan template ulasan. Setiap catatan yang ditambahkan diterapkan ke semua beban kerja yang menggunakan template ulasan, sedangkan tag khusus untuk template ulasan.

Untuk informasi lebih lanjut tentang tag, lihat [Memberikan tag ke sumber daya AWS WA Tool Anda](#).

5. Pilih Berikutnya.
6. Pada halaman Terapkan lensa, pilih lensa yang ingin Anda terapkan ke templat ulasan. Jumlah maksimum lensa yang dapat diterapkan adalah 20.

Lensa dapat dipilih dari lensa Kustom, Katalog Lensa, atau keduanya.


 Note

Lensa yang dibagikan dengan Anda tidak dapat diterapkan ke templat ulasan.

7. Pilih Buat templat.

Untuk mulai menjawab pertanyaan untuk template ulasan yang baru saja Anda buat

1. Pada tab Ikhtisar templat, di peringatan Mulai menjawab pertanyaan informasi, pilih lensa di menu tarik-turun Jawaban pertanyaan.

 Note

Anda juga dapat pergi ke bagian Lensa, pilih lensa, dan pilih Jawab pertanyaan.

2. Untuk setiap lensa yang telah Anda terapkan pada templat ulasan Anda, jawab pertanyaan yang berlaku dan pilih Simpan dan keluar setelah selesai.

Setelah template ulasan Anda dibuat, Anda dapat menentukan beban kerja baru darinya.

Tab Ikhtisar templat ulasan harus mencerminkan jumlah total Pertanyaan yang dijawab di bagian Detail Templat, dan Pertanyaan yang dijawab untuk setiap lensa di bagian Lensa.


Mengedit template ulasan di AWS WA Tool

Untuk mengedit template ulasan

1. Pilih Tinjau templat di panel navigasi kiri.
2. Pilih nama template ulasan yang ingin Anda edit.
3. Untuk memperbarui catatan Nama, Deskripsi, atau Templat untuk templat ulasan, pilih Edit di bagian Detail templat di tab Ikhtisar.
 - a. Buat perubahan pada catatan Nama, Deskripsi, atau Templat.
 - b. Pilih Simpan template untuk memperbarui template ulasan dengan perubahan Anda.
4. Untuk memperbarui lensa mana yang diterapkan pada templat ulasan, di bagian Lensa pada tab Ikhtisar, pilih Edit lensa yang diterapkan.

- a. Pilih atau batalkan pilihan kotak centang lensa yang ingin Anda tambahkan atau hapus.

Lensa dapat dipilih atau tidak dipilih dari lensa Kustom, Katalog Lensa, atau keduanya.
 - b. Pilih Simpan template untuk menyimpan perubahan Anda.
5. Untuk memperbarui jawaban atas pertanyaan praktik terbaik pada lensa, di bagian Lensa pada tab Ikhtisar, pilih nama lensa.
- a. Di bagian Ikhtisar lensa, pilih Jawab pertanyaan.

 **Note**

Secara opsional, Anda dapat memilih nama lensa di bawah menu tarik-turun Templat ulasan di panel navigasi kiri untuk membuka bagian Ikhtisar lensa.

- b. Pilih atau batalkan pilihan kotak centang di samping jawaban praktik terbaik yang ingin Anda ubah.
- c. Pilih Simpan dan keluar untuk menyimpan perubahan Anda.

Berbagi template ulasan di AWS WA Tool

Templat ulasan dapat dibagikan dengan pengguna atau akun, atau dapat dibagikan dengan seluruh organisasi atau unit organisasi.

Untuk berbagi template ulasan

1. Pilih Tinjau templat di panel navigasi kiri.
2. Pilih nama template ulasan yang ingin Anda bagikan.
3. Pilih tab Berbagi.
4. Untuk berbagi ke pengguna atau akun, pilih Buat dan pilih Bagikan dengan IAM pengguna atau akun. Di kotak Kirim undangan, tentukan pengguna atau akunIDs, dan pilih Buat.
5. Untuk berbagi ke organisasi atau unit organisasi, pilih Buat dan pilih Bagikan dengan Organizations. Untuk berbagi ke seluruh organisasi, pilih Berikan izin ke seluruh Organisasi. Untuk berbagi dengan unit organisasi, pilih Berikan izin ke Unit Organisasi individual, tentukan unit organisasi di kotak, dan pilih Buat.

⚠ Important

Sebelum berbagi profil dengan organisasi atau unit organisasi (OU), Anda harus [mengaktifkan AWS Organizations akses](#).

Mendefinisikan beban kerja dari template di AWS WA Tool

Anda dapat menentukan beban kerja dari template ulasan yang Anda buat atau template ulasan yang telah dibagikan dengan Anda. Anda tidak dapat menentukan beban kerja baru dari templat ulasan yang telah dihapus, dan jika templat peninjauan berisi versi lensa yang sudah ketinggalan zaman, Anda harus memutakhirkan templat peninjauan sebelum dapat menentukan beban kerja baru darinya. Untuk informasi tentang cara memutakhirkan templat ulasan, lihat [the section called "Meningkatkan lensa"](#).

ℹ Note

Untuk menentukan beban kerja dari templat ulasan, Anda harus memiliki IAM izin untuk mengaktifkan beban kerja:wellarchitected:CreateWorkload, serta izin templat tinjauan berikut:wellarchitected:GetReviewTemplate,, wellarchitected:GetReviewTemplateAnswer dan. wellarchitected:ListReviewTemplateAnswers wellarchitected:GetReviewTemplateLensReview Untuk informasi selengkapnya tentang IAM izin, lihat [Panduan AWS Identity and Access Management Pengguna](#).

Untuk menentukan beban kerja dari template ulasan

1. Pilih Tinjau templat di panel navigasi kiri.
2. Pilih nama template ulasan yang ingin Anda tentukan dari beban kerja.
3. Pilih Tentukan beban kerja dari template.

ℹ Note

Anda juga dapat memilih Tentukan dari template ulasan dari menu tarik-turun Tentukan beban kerja di halaman Beban kerja.

4. Pada langkah Pilih templat ulasan, pilih kartu templat ulasan, dan pilih Berikutnya.
5. Pada langkah Tentukan properti, isi bidang yang diperlukan untuk properti beban kerja, dan pilih Berikutnya. Untuk detail selengkapnya, lihat [the section called “Menentukan beban kerja”](#).
6. (Opsional) Pada langkah Terapkan Profil, kaitkan profil dengan beban kerja dengan memilih profil yang ada, mencari nama profil, atau memilih Buat profil untuk [membuat profil](#). Pilih Berikutnya.

Profil [Well-Architected](#) dan template ulasan dapat digunakan bersama-sama. Pertanyaan-pertanyaan yang telah diisi sebelumnya dalam template ulasan Anda tetap terjawab dalam beban kerja, dan pertanyaan diprioritaskan berdasarkan profil Anda.

7. (Opsional) Pada langkah Terapkan lensa, Anda dapat memilih untuk menerapkan lensa tambahan dari lensa Kustom atau katalog Lensa yang belum diterapkan pada templat ulasan.
8. Pilih Tentukan beban kerja.

Menghapus template ulasan di AWS WA Tool

Untuk menghapus template ulasan

1. Pilih Tinjau templat di panel navigasi kiri.
2. Di bagian Review templates, pilih template review yang ingin Anda hapus dan di dropdown Actions, pilih Delete.

Note

Anda juga dapat memilih nama templat dan memilih Hapus dari tab Ikhtisar templat ulasan.

3. Dalam kotak dialog Hapus templat ulasan, masukkan nama templat ulasan di bidang untuk mengonfirmasi penghapusan.
4. Pilih Hapus.

Anda tidak dapat membuat beban kerja baru dari template ulasan yang telah dihapus. Jika Anda telah membagikan templat ulasan yang Anda hapus dengan IAM pengguna, akun, atau organisasi lain, mereka tidak akan dapat membuat beban kerja darinya.

Menggunakan profil di AWS WA Tool

Anda dapat membuat profil untuk memberikan konteks pada bisnis Anda, serta mengidentifikasi tujuan yang ingin Anda capai saat melakukan tinjauan Well-Architected. AWS Well-Architected Tool menggunakan informasi yang dikumpulkan dari profil Anda untuk membantu Anda fokus pada daftar pertanyaan yang diprioritaskan yang relevan dengan bisnis Anda selama tinjauan beban kerja. Dengan melampirkan profil ke beban kerja, Anda bisa melihat risiko mana saja yang diprioritaskan untuk Anda atasi dengan rencana perbaikan Anda.

Anda dapat [membuat profil](#) dari halaman Profil dan mengaitkannya dengan beban kerja baru, atau Anda dapat [menambahkan profil ke beban kerja yang sudah ada](#).

Membuat profil

Untuk membuat profil

1. Pilih Profil di panel navigasi kiri.
2. Pilih Buat profil.
3. Di bagian Properti profil, masukkan Nama dan Deskripsi untuk profil Anda.
4. Untuk menyempurnakan informasi yang diprioritaskan untuk bisnis Anda dalam tinjauan beban kerja dan rencana perbaikan, pilih jawaban yang paling relevan dengan bisnis Anda di bagian Pertanyaan profil.
5. (Opsional) Di bagian Tag, tambahkan tag yang ingin Anda kaitkan dengan profil.

Untuk informasi selengkapnya tentang tag, lihat [Memberikan tag ke sumber daya AWS WA Tool Anda](#).

6. Pilih Simpan. Pesan berhasil akan muncul ketika profil berhasil dibuat.

Saat profil dibuat, ikhtisar profil akan ditampilkan. Ikhtisar menunjukkan data yang dikaitkan dengan profil, termasuk nama, deskripsi, ARN, tanggal dibuat dan diperbarui, dan jawaban atas pertanyaan profil. Dari halaman ikhtisar profil, Anda dapat mengedit, menghapus, atau membagikan profil Anda.

Mengedit profil di AWS WA Tool

Untuk mengedit profil

1. Pilih Profil di panel navigasi kiri, atau pilih Lihat profil dari bagian Profil pada beban kerja.
2. Pilih nama profil yang ingin Anda perbarui.
3. Pilih Edit di halaman Ikhtisar profil.
4. Buat pembaruan yang diperlukan pada pertanyaan profil.
5. Pilih Simpan.

Berbagi profil di AWS WA Tool

Profil dapat dibagikan dengan pengguna atau akun, atau dapat dibagikan dengan seluruh organisasi atau unit organisasi.

Untuk berbagi profil

1. Pilih Profil di panel navigasi kiri.
2. Pilih nama profil yang ingin Anda bagikan.
3. Pilih tab Berbagi.
4. Untuk berbagi ke pengguna atau akun, pilih Buat dan pilih Buat pembagian ke pengguna atau akun IAM. Di kotak Kirim undangan, tentukan ID pengguna atau akun, lalu pilih Buat.
5. Untuk berbagi ke organisasi atau unit organisasi, pilih Buat dan pilih Buat pembagian ke Organisasi. Untuk berbagi ke seluruh organisasi, pilih Berikan izin ke seluruh Organisasi. Untuk berbagi dengan unit organisasi, pilih Berikan izin ke Unit Organisasi individual, tentukan unit organisasi di kotak, lalu pilih Buat.

Important

Sebelum membagikan profil ke organisasi atau unit organisasi (OU), Anda harus [mengaktifkan akses AWS Organizations](#).

Menambahkan profil ke beban kerja di AWS WA Tool

Anda dapat menambahkan profil ke beban kerja yang ada, atau saat menentukan beban kerja, untuk mempercepat proses tinjauan beban kerja. AWS WA Tool menggunakan informasi yang dikumpulkan dari profil Anda untuk memprioritaskan pertanyaan dalam tinjauan beban kerja yang relevan dengan bisnis Anda.

Untuk informasi selengkapnya tentang menambahkan profil saat menentukan beban kerja, lihat [the section called “Menentukan beban kerja”](#).

Untuk menambahkan profil ke beban kerja yang sudah ada

1. Pilih Beban kerja di panel navigasi kiri, dan pilih nama beban kerja yang ingin Anda kaitkan dengan profil.

Note

Hanya satu profil yang dapat dikaitkan dengan beban kerja.

2. Di bagian Profil, pilih Tambahkan profil.
3. Pilih profil yang ingin Anda terapkan ke beban kerja dari daftar profil yang tersedia, atau pilih Buat profil. Untuk informasi selengkapnya, lihat [the section called “Membuat profil”](#).
4. Pilih Simpan.

Ikhtisar Beban Kerja menampilkan hitungan pertanyaan prioritas yang dijawab dan risiko yang diprioritaskan berdasarkan informasi di profil terkait. Pilih Lanjutkan meninjau untuk menjawab pertanyaan yang diprioritaskan dalam tinjauan beban kerja. Untuk informasi selengkapnya, lihat [the section called “Mendokumentasikan beban kerja”](#).

Bagian Profil menampilkan nama, deskripsi, ARN, versi, dan tanggal terakhir diperbarui untuk profil yang terkait dengan beban kerja.

Menghapus profil dari beban kerja di AWS WA Tool

Menghapus profil dari beban kerja akan mengembalikan beban kerja ke versi sebelum profil dikaitkan dengannya, dan pertanyaan serta risiko tinjauan beban kerja tidak lagi diprioritaskan.

Untuk menghapus profil dari beban kerja

1. Dari bagian Profil beban kerja, pilih Hapus.
2. Untuk mengonfirmasi penghapusan, masukkan nama profil di dalam bidang input teks.
3. Pilih Hapus.

Notifikasi bahwa profil telah berhasil dihapus dari beban kerja akan ditampilkan. Menghapus profil akan mengembalikan beban kerja ke versi sebelum profil dikaitkan dengannya, dan pertanyaan serta risiko tinjauan beban kerja tidak lagi diprioritaskan.

Menghapus profil dari AWS WA Tool

Jika Anda membuat profil, Anda dapat menghapus profil dari daftar profil yang tersedia di AWS WA Tool.

Menghapus profil dari halaman Profil tidak menghapus profil dari beban kerja terkait. Anda dapat terus menggunakan profil yang dibagikan dan dikaitkan dengan beban kerja sebelum penghapusan, namun, tidak ada beban kerja baru yang dapat dikaitkan dengan profil yang dihapus. [the section called “Pemberitahuan profil”](#) dikirim ke pemilik beban kerja menggunakan profil yang dihapus.

Penafian

Dengan membagikan profil Anda ke Akun AWS lain, Anda mengonfirmasi bahwa AWS akan membuat profil Anda tersedia untuk akun lain tersebut. Akun lain tersebut dapat terus mengakses dan menggunakan profil yang dibagikan meskipun Anda menghapus profil tersebut dari Akun AWS Anda sendiri atau mengakhiri Akun AWS Anda.

Untuk menghapus profil dari daftar profil Anda

1. Pilih Profil di panel navigasi kiri.
2. Pilih nama pengguna yang ingin Anda hapus.
3. Pilih Hapus.
4. Untuk mengonfirmasi penghapusan, masukkan nama profil di dalam bidang input teks.
5. Pilih Hapus.

Jika Anda ingin mempertahankan profil di daftar Profil Anda, tetapi menghapusnya dari beban kerja, lihat [the section called “Menghapus profil dari beban kerja”](#).

AWS Well-Architected Tool Konektor untuk Jira

Anda dapat menggunakan AWS Well-Architected Tool Connector for Jira untuk menautkan akun Jira Anda dengan AWS Well-Architected Tool dan menyinkronkan item peningkatan dari beban kerja Anda ke proyek Jira untuk membantu Anda membuat mekanisme loop tertutup dalam menerapkan peningkatan.

Konektor menyediakan sinkronisasi Otomatis dan Manual. Untuk detail selengkapnya, lihat [Mengkonfigurasi konektor](#).

Konektor dapat diatur di tingkat akun dan tingkat beban kerja, dengan opsi untuk mengganti pengaturan tingkat akun Anda per beban kerja. Pada tingkat beban kerja, Anda juga dapat memilih untuk mengecualikan beban kerja dari sinkronisasi sepenuhnya.

Anda dapat memilih untuk menyinkronkan item perbaikan ke proyek WA Jira default, atau menentukan kunci proyek yang ada untuk disinkronkan. Pada tingkat beban kerja, Anda dapat menyinkronkan setiap beban kerja ke proyek Jira yang unik jika perlu.

Note

Konektor hanya mendukung proyek scrum dan kanban di Jira.

Ketika item perbaikan disinkronkan ke Jira, mereka diatur dengan cara berikut:

- Proyek: WA (atau proyek yang ada yang Anda tentukan)
- Epic: Beban Kerja
- Tugas: Pertanyaan
- Sub-tugas: Praktik terbaik
- Label: Pilar

Setelah Anda mengatur sinkronisasi akun Jira di halaman Pengaturan, Anda dapat [mengonfigurasi konektor Jira](#) dan [menyinkronkan item peningkatan ke akun Jira Anda](#).

Menyiapkan konektor

Untuk memasang konektor

Note

Semua langkah berikut dilakukan di akun Jira Anda, bukan di akun Anda Akun AWS.

1. Masuk ke akun Jira Anda.
2. Di bilah navigasi atas, pilih Aplikasi, lalu pilih Jelajahi aplikasi lainnya.
3. Di halaman Temukan aplikasi dan integrasi untuk Jira, masukkan AWS Well-Architected. Kemudian, pilih AWS Well-Architected Tool Connector untuk JIRA.
4. Di halaman aplikasi, pilih Dapatkan aplikasi.
5. Di panel Tambahkan ke Jira, pilih Dapatkan sekarang.
6. Setelah aplikasi diinstal, untuk menyelesaikan penyiapan, pilih Konfigurasi.
7. Di halaman AWS Well-Architected Tool Konfigurasi, pilih Connect a new Akun AWS.
8. Masukkan AccessKeyID dan Kunci Rahasia Anda. Opsional: Masukkan Token Sesi Anda. Kemudian, pilih Connect.

Note

Pastikan akun Anda memiliki izin `wellarchitected:ConfigureIntegration`. Izin ini diperlukan untuk ditambahkan Akun AWS ke Jira.
Beberapa Akun AWS dapat dihubungkan ke AWS WA Tool.

Note

Sebagai praktik terbaik keamanan, sangat disarankan untuk menggunakan kredensial IAM jangka pendek. Untuk detail tentang cara membuat AccessKeyID dan Kunci Rahasia untuk Anda Akun AWS, lihat [Mengelola kunci akses \(konsol\)](#), dan untuk detail tentang penggunaan kredensial jangka pendek, lihat [Meminta](#) kredensial sementara.

9. Untuk Wilayah, pilih yang ingin Region AWS Anda sambungkan. Kemudian, pilih Connect.

Pengaturan proyek Jira

Saat menggunakan proyek khusus, pastikan Anda memiliki jenis masalah berikut dalam pengaturan proyek Anda:

- Scrum: Epik, Cerita, Subtugas
- Kanban: Epik, Tugas, Subtugas

Untuk detail tentang mengelola jenis masalah, lihat [Atlassian Support | Menambahkan, mengedit, dan menghapus jenis masalah](#).

Untuk memeriksa status konektor di AWS Well-Architected Tool

1. Masuk ke Anda Akun AWS dan navigasikan ke AWS Well-Architected Tool.
2. Pilih Pengaturan di panel navigasi kiri.
3. Di bagian sinkronisasi akun Jira, di bawah status koneksi aplikasi Jira, periksa status Dikonfigurasi.

Konektor sekarang diatur dan siap untuk dikonfigurasi. Untuk mengonfigurasi pengaturan sinkronisasi JIRA di tingkat akun dan beban kerja, lihat [Mengonfigurasi konektor](#).

Mengkonfigurasi konektor

Dengan AWS Well-Architected Tool Konektor untuk Jira, Anda dapat mengonfigurasi sinkronisasi Jira di tingkat akun, tingkat beban kerja, atau keduanya. Anda dapat mengonfigurasi setelan Jira tingkat beban kerja secara independen dari setelan tingkat akun, atau mengganti setelan tingkat akun pada beban kerja tertentu untuk menentukan perilaku sinkronisasi beban kerja. Anda juga dapat mengonfigurasi pengaturan JIRA saat [Mendefinisikan beban kerja](#).

Konektor menyediakan dua metode sinkronisasi: Sinkronisasi otomatis dan Manual. Dalam kedua metode sinkronisasi, perubahan yang dibuat AWS WA Tool tercermin dalam proyek Jira Anda, dan perubahan yang dibuat di Jira disinkronkan kembali ke AWS WA Tool

Important


Dengan menggunakan Sinkronisasi otomatis, Anda setuju untuk AWS WA Tool memodifikasi beban kerja Anda sebagai respons terhadap perubahan di Jira.

Jika Anda memiliki informasi sensitif yang tidak ingin Anda sinkronkan ke Jira, jangan masukkan informasi ini ke bidang Catatan di beban kerja Anda.

- Sinkronisasi otomatis: Konektor secara otomatis memperbarui proyek Jira Anda dan beban kerja Anda setiap kali pertanyaan diperbarui, termasuk memilih atau membatalkan pilihan praktik terbaik dan menyelesaikan pertanyaan.
- Sinkronisasi manual: Anda harus memilih Sinkronkan dengan Jira di dasbor beban kerja saat Anda ingin menyinkronkan item peningkatan antara Jira dan AWS WA Tool Anda juga dapat memilih pilar dan pertanyaan spesifik mana yang ingin Anda sinkronkan. Untuk detail selengkapnya, lihat [Menyinkronkan beban kerja](#).

Untuk mengkonfigurasi konektor di tingkat akun

1. Pilih Pengaturan di panel navigasi kiri.
2. Di panel sinkronisasi akun Jira, pilih Edit.
3. Untuk jenis Sinkronisasi, pilih salah satu dari berikut ini:
 - a. Untuk menyinkronkan beban kerja secara otomatis saat perubahan dilakukan, pilih Otomatis.
 - b. Untuk memilih secara manual kapan harus menyinkronkan beban kerja, pilih Manual.
4. Secara default, konektor membuat proyek WA Jira. Untuk menentukan kunci proyek Jira Anda sendiri, lakukan hal berikut:
 - a. Pilih Ganti kunci proyek Jira default.
 - b. Masukkan kunci proyek Jira Anda.

 Note

Kunci proyek JIRA yang ditentukan digunakan untuk semua beban kerja kecuali Anda mengubah proyek pada tingkat beban kerja.

5. Pilih Simpan pengaturan.

Untuk mengkonfigurasi konektor pada tingkat beban kerja

1. Pilih Beban kerja di panel navigasi kiri, dan pilih nama beban kerja yang ingin Anda konfigurasi.
2. Pilih Properti.
3. Di panel Jira, pilih Edit.
4. Untuk mengonfigurasi pengaturan Jira beban kerja, pilih Ganti pengaturan tingkat akun.

Note

Mengganti pengaturan level akun harus dipilih untuk menerapkan pengaturan khusus beban kerja.

5. Untuk penggantian Sinkronisasi, pilih salah satu dari berikut ini:
 - a. Untuk mengecualikan beban kerja dari sinkronisasi JIRA, pilih Jangan sinkronkan beban kerja.
 - b. Untuk memilih secara manual kapan harus menyinkronkan beban kerja, pilih Sinkronkan beban kerja - Manual.
 - c. Untuk menyinkronkan perubahan beban kerja secara otomatis, pilih Sinkronkan beban kerja - Otomatis.
6. (Opsional) Untuk kunci proyek Jira, masukkan kunci proyek untuk menyinkronkan beban kerja. Kunci proyek ini dapat berbeda dari kunci proyek tingkat akun Anda.

Jika Anda tidak menentukan kunci proyek, konektor akan membuat proyek WA Jira.

7. Pilih Simpan.

Untuk detail tentang melakukan sinkronisasi manual, lihat [Menyinkronkan beban kerja](#).

Menyinkronkan beban kerja

Untuk Sinkronisasi otomatis, konektor secara otomatis menyinkronkan item peningkatan saat Anda memperbarui beban kerja (misalnya, saat Anda menyelesaikan pertanyaan atau memilih praktik terbaik baru).

Dalam sinkronisasi Manual dan Otomatis, setiap perubahan yang dibuat di Jira (seperti menyelesaikan pertanyaan atau praktik terbaik) disinkronkan kembali ke AWS Well-Architected Tool

Untuk menyinkronkan beban kerja secara manual

1. Saat Anda siap untuk menyinkronkan beban kerja Anda ke Jira, pilih Beban kerja di panel navigasi kiri. Kemudian, pilih beban kerja yang ingin Anda sinkronkan.
2. Dalam ikhtisar beban kerja, pilih Sinkronkan dengan Jira.
3. Pilih lensa yang ingin Anda sinkronkan.
4. Untuk Pertanyaan untuk disinkronkan ke Jira, pilih pertanyaan atau seluruh pilar yang ingin Anda sinkronkan ke proyek Jira.
 - Untuk pertanyaan yang ingin Anda hapus, pilih ikon X di sebelah judul pertanyaan.
5. Pilih Sinkronisasi.

Menghapus pemasangan konektor

Untuk menghapus sepenuhnya AWS Well-Architected Tool Konektor untuk Jira, lakukan tugas-tugas berikut:

- Matikan sinkronisasi Jira di beban kerja apa pun yang menimpa setelah sinkronisasi tingkat akun
- Matikan sinkronisasi Jira di tingkat akun
- Putuskan tautan Anda Akun AWS di Jira
- Copot pemasangan konektor dari akun Jira Anda

Untuk mematikan konektor di tingkat akun

Note

Langkah-langkah berikut dilakukan di Anda Akun AWS.

1. Pilih Pengaturan di panel navigasi kiri.
2. Di bagian sinkronisasi akun JIRA, pilih Edit.
3. Hapus opsi Aktifkan sinkronisasi akun Jira.
4. Pilih Simpan pengaturan.

Untuk memutuskan tautan Akun AWS

Note

Semua langkah berikut dilakukan di akun Jira Anda, bukan di akun Anda Akun AWS.

1. Masuk ke akun Jira Anda.
2. Di bilah navigasi atas, pilih Aplikasi, lalu pilih Kelola aplikasi Anda.
3. Pilih panah tarik-turun di sebelah AWS Well-Architected Tool Connector for Jira, lalu pilih Configure.
4. Di panel AWS Well-Architected Tool Konfigurasi, untuk memutuskan tautan Akun AWS, pilih X di bawah Tindakan.

Untuk mencopot pemasangan konektor

Note

Semua langkah berikut dilakukan di akun Jira Anda, bukan di akun Anda Akun AWS. Sebaiknya verifikasi bahwa semua yang Akun AWS terhubung tidak terhubung dalam konfigurasi konektor sebelum mencopot pemasangan konektor.

1. Masuk ke akun Jira Anda.
2. Di bilah navigasi atas, pilih Aplikasi, lalu pilih Kelola aplikasi Anda.
3. Pilih panah tarik-turun di sebelah AWS Well-Architected Tool Konektor untuk Jira.
4. Pilih Uninstall, lalu pilih Uninstall app.

Tonggak sejarah

Tonggak sejarah mencatat keadaan beban kerja pada titik waktu tertentu.

Simpan tonggak sejarah setelah Anda menyelesaikan semua pertanyaan yang terkait dengan beban kerja. Ketika Anda mengubah beban kerja Anda berdasarkan item dalam rencana perbaikan Anda, Anda dapat menyimpan tonggak tambahan untuk mengukur kemajuan.

Praktik terbaik adalah menyimpan tonggak sejarah setiap kali Anda melakukan perbaikan pada beban kerja.

Menyimpan tonggak

Tonggak sejarah mencatat keadaan beban kerja saat ini. Pemilik beban kerja dapat menyimpan tonggak sejarah kapan saja.

Untuk menyimpan tonggak sejarah

1. Dari halaman detail beban kerja, pilih **Simpan tonggak**.
2. Di **Nama tonggak** kotak, masukkan nama untuk tonggak Anda.

Note

Nama harus berkisar antara 3 sampai 100 karakter. Setidaknya tiga karakter tidak boleh spasi. Nama tonggak yang terkait dengan beban kerja harus unik. Spasi dan kapitalisasi diabaikan saat memeriksa keunikan.

3. Pilih **Simpan** untuk menyelamatkan tonggak sejarah.

Setelah tonggak disimpan, Anda tidak dapat mengubah data beban kerja yang direkam. Jika Anda menghapus beban kerja, tonggak terkait juga dihapus.

Melihat tonggak

Anda dapat melihat tonggak untuk beban kerja dengan cara berikut:

- Pada halaman rincian beban kerja, pilih **Tonggak sejarah** dan pilih tonggak yang ingin Anda lihat.

- PadaDasborhalaman, pilih beban kerja dan diTonggak sejarahbagian, pilih tonggak yang ingin Anda lihat.

Menghasilkan laporan tonggak

Anda dapat membuat laporan tonggak sejarah. Laporan berisi tanggapan terhadap pertanyaan beban kerja, catatan Anda, dan risiko tinggi dan menengah yang hadir saat tonggak disimpan.

Sebuah laporan memungkinkan Anda untuk berbagi rincian tentang tonggak sejarah dengan orang lain yang tidak memiliki akses keAWS Well-Architected Tool.

Untuk menghasilkan laporan tonggak

1. Pilih tonggak dengan salah satu cara berikut.
 - Dari halaman detail beban kerja, pilihTonggak sejarahdan memilih tonggak sejarah.
 - DariDasborhalaman, pilih beban kerja dengan tonggak yang ingin Anda laporkan. DiTonggak sejarahbagian, pilih tonggak sejarah.
2. PilihBuat laporanuntuk membuat laporan.

File PDF dihasilkan dan Anda dapat mengunduh atau melihatnya.

Bagikan undangan

Undangan berbagi adalah permintaan untuk membagikan beban kerja, lensa khusus, atau templat ulasan yang dimiliki oleh AWS akun lain. Beban kerja atau lensa dapat dibagi dengan semua pengguna dalam satu Akun AWS, pengguna individu, atau keduanya.

- Jika Anda menerima undangan beban kerja, beban kerja akan ditambahkan ke halaman Beban Kerja dan Dasbor Anda.
- Jika Anda menerima undangan lensa khusus, lensa ditambahkan ke halaman lensa Kustom Anda.
- Jika Anda menerima undangan profil, profil akan ditambahkan ke halaman Profil Anda.
- Jika Anda menerima undangan templat ulasan, templat akan ditambahkan ke halaman templat Ulasan Anda.

Jika Anda menolak undangan, itu dihapus dari daftar.

Note

Beban kerja, lensa khusus, profil, dan templat ulasan hanya dapat dibagi dalam hal yang sama AWS Region.

Pemilik beban kerja atau lensa kustom mengontrol siapa yang memiliki akses bersama.

Halaman Bagikan undangan, tersedia dari navigasi kiri, memberikan informasi tentang beban kerja Anda yang tertunda dan undangan lensa kustom.

Informasi berikut ditampilkan untuk setiap undangan beban kerja:

Nama

Nama beban kerja, lensa kustom, atau template ulasan yang akan dibagikan.

Tipe sumber daya

Jenis undangan, baik Workload, Custom lens, Profiles, atau Review Template.

Pemilik

Akun AWSID yang memiliki beban kerja.

Izin

Izin bahwa Anda diberikan untuk beban kerja.

- Hanya Baca

Menyediakan akses hanya-baca ke beban kerja, lensa kustom, profil, atau template ulasan.

- Kontributor

Menyediakan akses pembaruan ke jawaban dan catatannya, dan akses hanya-baca ke sisa beban kerja. Izin ini hanya tersedia untuk beban kerja.

Detail izin

Deskripsi terperinci tentang izin.

Menerima undangan berbagi

Untuk menerima undangan berbagi

1. Pilih undangan berbagi untuk menerima.
2. Pilih Terima.

Untuk undangan beban kerja, beban kerja ditambahkan ke halaman Beban Kerja dan Dasbor. Untuk undangan lensa kustom, lensa kustom ditambahkan ke halaman Lensa kustom. Untuk undangan profil, profil ditambahkan ke halaman Profil. Untuk undangan template ulasan, template ditambahkan ke halaman Template ulasan.

Anda memiliki tujuh hari untuk menerima undangan. Jika Anda tidak menerima undangan dalam waktu tujuh hari, itu akan kedaluwarsa secara otomatis.

Jika pengguna dan Akun AWS keduanya telah menerima undangan beban kerja, undangan beban kerja untuk pengguna menentukan izin pengguna.

Menolak undangan berbagi

Untuk menolak undangan berbagi

1. Pilih beban kerja atau undangan lensa khusus untuk ditolak.

2. Pilih Tolak.

Undangan dihapus dari daftar.

Notifikasi

Halaman Notifikasi menampilkan perbedaan versi untuk beban kerja dan templat ulasan yang memiliki lensa dan profil yang terkait dengannya. Anda dapat meningkatkan ke versi terbaru lensa atau profil untuk beban kerja dari halaman Pemberitahuan.

Pemberitahuan lensa

Ketika versi baru lensa tersedia, spanduk muncul di bagian atas halaman Workloads atau Review template untuk memberi tahu Anda. Jika Anda melihat beban kerja atau templat ulasan tertentu menggunakan lensa yang sudah ketinggalan zaman, Anda juga akan melihat spanduk yang menunjukkan bahwa versi lensa baru tersedia.

Pilih Lihat peningkatan yang tersedia untuk daftar beban kerja atau templat ulasan yang dapat ditingkatkan.

Lihat [the section called “Meningkatkan lensa”](#) petunjuk tentang memutakhirkan lensa untuk beban kerja atau templat ulasan.

Ketika pemilik lensa bersama menghapusnya, jika Anda memiliki beban kerja yang terkait dengan lensa yang dihapus, Anda akan menerima pemberitahuan bahwa Anda masih dapat menggunakan lensa di beban kerja yang ada, tetapi Anda tidak akan dapat menambahkannya ke beban kerja baru.

Pemberitahuan profil

Ada dua jenis pemberitahuan Profil:

- Peningkatan profil
- Penghapusan profil

Ketika profil yang terkait dengan beban kerja telah diedit (untuk informasi selengkapnya, lihat [the section called “Mengedit profil”](#)), pemberitahuan bahwa ada versi baru profil ditampilkan di Pemberitahuan profil.

Ketika pemilik profil bersama menghapusnya, jika Anda memiliki beban kerja yang terkait dengan profil yang dihapus, Anda akan menerima pemberitahuan bahwa Anda masih dapat menggunakan

profil di beban kerja Anda yang ada, tetapi Anda tidak akan dapat menambahkannya ke beban kerja baru.

Untuk meng-upgrade versi profil

1. Di panel navigasi kiri, pilih Pemberitahuan.
2. Pilih nama beban kerja dari daftar di tab Pemberitahuan profil, atau gunakan bilah pencarian untuk mencari berdasarkan nama beban kerja.
3. Pilih versi profil upgrade.
4. Di bagian Pengakuan, pilih kotak konfirmasi untuk saya mengerti dan menerima perubahan ini.
5. (Opsional) Jika memilih untuk menyimpan tonggak sejarah, pilih kotak Simpan tonggak sejarah dan berikan nama Milestone.
6. Pilih Simpan.

Setelah profil ditingkatkan, nomor versi terbaru dan tanggal diperbarui ditampilkan di bagian Profil dari beban kerja.

Lihat [Profil](#) untuk informasi selengkapnya.

Dasbor

Dasbor, tersedia dari navigasi kiri, memberi Anda akses ke beban kerja Anda dan masalah risiko menengah dan tinggi terkait. Anda juga dapat menyertakan beban kerja yang telah dibagikan dengan Anda. Dasbor terdiri dari empat bagian.

- Ringkasan - Menunjukkan jumlah total beban kerja, berapa banyak yang memiliki risiko tinggi dan menengah, dan jumlah total masalah risiko tinggi dan menengah di semua beban kerja.
- Masalah Kerangka Kerja yang Didesain dengan Baik per pilar - Menunjukkan representasi grafis dari masalah risiko tinggi dan menengah berdasarkan pilar untuk semua beban kerja Anda.
- Masalah Kerangka Kerja yang Didesain dengan Baik per beban kerja - Menunjukkan masalah risiko tinggi dan menengah berdasarkan pilar untuk setiap beban kerja Anda.
- Masalah Kerangka Kerja yang Didesain dengan Baik berdasarkan item rencana perbaikan - Menunjukkan item rencana perbaikan untuk semua beban kerja Anda.

Ringkasan

Bagian ini menunjukkan jumlah total beban kerja dan jumlah beban kerja dengan masalah risiko tinggi dan menengah di seluruh lensa Well-Architected Framework dan semua lensa lainnya. Jumlah total masalah risiko tinggi dan menengah di semua beban kerja, baik yang dimiliki oleh atau dibagikan dengan AndaAkun AWS, ditampilkan.

Pilih Sertakan beban kerja yang dibagikan kepada saya agar statistik ringkasan, laporan konsolidasi, dan bagian dasbor lainnya mencerminkan beban kerja dan beban kerja Anda yang telah dibagikan dengan Anda.

Pilih Buat laporan agar laporan konsolidasi dibuat untuk Anda sebagai file PDF.

Nama laporannya berupa: `wellarchitected_consolidatedreport_`*account-ID*.pdf.

Masalah Kerangka Kerja yang Dirancang dengan Baik per Pilar

Masalah Kerangka Kerja Well-Architected per bagian pilar menunjukkan representasi grafis dari jumlah masalah risiko tinggi dan menengah berdasarkan pilar untuk semua beban kerja.

Gunakan bagian dashboard yang tersisa untuk berpindah dari satu tingkat detail ke tingkat berikutnya.

Note

Hanya masalah dari lensa Well-Architected Framework yang disertakan dalam bagian ini.

Masalah Kerangka Kerja yang Dirancang dengan Baik per Beban Kerja

Masalah Kerangka Kerja Well-Architected per bagian beban kerja menampilkan informasi untuk setiap beban kerja.

Name	Total issues	Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization	Sustainability	Last updated
Retail Website - EU Questions answered: 46/46 Lenses applied: 1	High: 15 Medium: 11	High: 0 Medium: 5	High: 1 Medium: 0	⊕ High: 7 Medium: 1	High: 5 Medium: 1	High: 2 Medium: 4	High: 0 Medium: 0	Mar 15, 2023 12:31 PM UTC-6

Informasi berikut ini ditampilkan untuk masing-masing beban kerja:

Nama

Nama beban kerja. Jumlah pertanyaan yang dijawab, dan jumlah lensa yang diterapkan pada beban kerja juga ditampilkan.

Pilih nama beban kerja untuk mengunjungi halaman detail beban kerja dan melihat tonggak sejarah, rencana perbaikan, dan berbagi.

Total masalah

Jumlah total masalah yang diidentifikasi oleh lensa Well-Architected Framework untuk beban kerja.

Pilih jumlah masalah risiko tinggi atau menengah untuk melihat rencana perbaikan yang disarankan untuk masalah tersebut.

Keunggulan Operasional

Jumlah masalah risiko tinggi (HRI) dan masalah risiko menengah (MRI) yang teridentifikasi dalam beban kerja untuk pilar Operational Excellence.

Keamanan

Jumlah HRI dan MRI yang diidentifikasi untuk pilar Keamanan.

Keandalan

Jumlah HRI dan MRI yang diidentifikasi untuk pilar Keandalan.

Kinerja Efisiensi

Jumlah HRI dan MRI yang diidentifikasi untuk pilar Efisiensi Kinerja.

Pengoptimalan Biaya

Jumlah HRI dan MRI yang diidentifikasi untuk pilar Optimasi Biaya.

Keberlanjutan

Jumlah HRI dan MRI yang diidentifikasi untuk pilar Keberlanjutan.

Terakhir diperbarui

Tanggal dan waktu beban kerja terakhir diperbarui.

Untuk setiap beban kerja, pilar dengan jumlah masalah risiko tinggi (HRI) tertinggi disorot.

Note

Hanya masalah dari lensa Well-Architected Framework yang disertakan dalam bagian ini.

Masalah Kerangka Kerja Well-Architected oleh item rencana perbaikan

Masalah Kerangka Kerja Well-Architected oleh bagian item rencana perbaikan menampilkan item rencana perbaikan untuk semua beban kerja Anda. Anda dapat memfilter item berdasarkan pilar dan tingkat keparahan.

Informasi berikut ini ditampilkan untuk masing-masing item rencana perbaikan:

Item perbaikan

Nama item rencana perbaikan.

Pilih nama untuk menunjukkan praktik terbaik yang terkait dengan item rencana perbaikan.

Pilar

Pilar yang terkait dengan item perbaikan.

Risiko

Menunjukkan apakah masalah terkait berisiko tinggi atau sedang.

Beban kerja yang berlaku

Jumlah beban kerja di mana rencana perbaikan ini berlaku.

Pilih item rencana perbaikan untuk melihat beban kerja yang berlaku.

Note

Hanya item rencana perbaikan dari lensa Well-Architected Framework yang disertakan dalam bagian ini.

Keamanan di AWS Well-Architected Tool

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

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

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan-layanan AWS di AWS Cloud. AWS juga memberikan Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi secara berkala efektivitas keamanan kami sebagai bagian dari [Program Kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku di AWS Well-Architected Tool, lihat [Layanan AWS dalam Cakupan menurut Program Kepatuhan](#).
- Keamanan di cloud – Tanggung jawab Anda ditentukan oleh layanan AWS yang digunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini akan membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS WA Tool. Topik berikut akan menunjukkan kepada Anda cara membuat konfigurasi AWS WA Tool untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan layanan AWS lain yang membantu Anda memantau dan mengamankan sumber daya AWS WA Tool Anda.

Topik

- [Perlindungan data di AWS Well-Architected Tool](#)
- [Manajemen identitas dan akses untuk AWS Well-Architected Tool](#)
- [Respons insiden di AWS Well-Architected Tool](#)
- [Validasi kepatuhan untuk AWS Well-Architected Tool](#)
- [Ketahanan di AWS Well-Architected Tool](#)
- [Keamanan infrastruktur di AWS Well-Architected Tool](#)
- [Analisis konfigurasi dan kerentanan dalam AWS Well-Architected Tool](#)
- [Pencegahan "confused deputy" lintas layanan](#)

Perlindungan data di AWS Well-Architected Tool

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

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

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya AWS. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan log aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan jalur CloudTrail untuk merekam aktivitas AWS, lihat [Bekerja dengan jalur CloudTrail](#) dalam Panduan Pengguna AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama semua kontrol keamanan default dalam 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 ketika 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 WA Tool atau layanan Layanan AWS lainnya dengan menggunakan konsol, API, AWS CLI, atau SDK AWS. 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.

Enkripsi saat diam

Semua data yang disimpan oleh AWS WA Tool dienkripsi saat diam.

Enkripsi saat bergerak

Semua data yang dikirim ke dan dari AWS WA Tool dienkripsi saat bergerak.

Cara AWS menggunakan data Anda

Tim AWS Well-Architected mengumpulkan data agregat dari AWS Well-Architected Tool untuk menyediakan dan meningkatkan layanan AWS WA Tool bagi pelanggan. Data pelanggan individual dapat dibagikan kepada tim Akun AWS untuk mendukung upaya pelanggan kami dalam meningkatkan beban kerja dan arsitektur mereka. Tim AWS Well-Architected hanya dapat mengakses properti beban kerja dan pilihan yang ditentukan untuk setiap pertanyaan. AWS tidak membagikan data apa pun dari AWS WA Tool di luar AWS.

Properti beban kerja yang dapat diakses oleh tim AWS Well-Architected termasuk:

- Nama beban kerja
- Pemilik peninjauan
- Lingkungan
- Wilayah
- ID akun
- Jenis Industri

Tim AWS Well-Architected tidak memiliki akses ke:

- Deskripsi beban kerja
- Desain arsitektur
- Catatan apa pun yang Anda masukkan

Manajemen identitas dan akses untuk AWS Well-Architected Tool

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengendalikan akses ke sumber daya AWS secara aman. Administrator IAM mengontrol siapa yang dapat terautentikasi (masuk) dan berwenang (memiliki izin) untuk menggunakan sumber daya AWS WA Tool. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa dikenai biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Cara kerja AWS Well-Architected Tool dengan IAM](#)
- [Contoh kebijakan berbasis identitas AWS Well-Architected Tool](#)
- [Kebijakan yang dikelola AWS untuk AWS Well-Architected Tool](#)
- [Pemecahan masalah identitas dan akses AWS Well-Architected Tool](#)

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 identitas dan akses AWS Well-Architected Tool](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Cara kerja AWS Well-Architected Tool dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Contoh kebijakan berbasis identitas AWS Well-Architected Tool](#))

Mengautentikasi dengan identitas

Autentikasi merupakan cara Anda untuk masuk ke AWS menggunakan kredensial identitas Anda. Anda harus terautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengambil peran IAM.

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

Untuk akses terprogram, AWS menyediakan 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

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

Identitas terfederasi

Sebagai praktik terbaik, wajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas guna mengakses Layanan AWS dengan kredensial sementara.

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

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

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Wajibkan pengguna manusia menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensial sementara](#) dalam 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 API AWS. 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 mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Sebuah kebijakan menentukan izin saat dikaitkan dengan sebuah identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika principal mengajukan permintaan. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

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

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

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

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

Jenis-jenis kebijakan lain

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

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations.
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCP\)](#) dalam Panduan Pengguna AWS Organizations.
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

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

Cara kerja AWS Well-Architected Tool dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke AWS WA Tool, Anda harus memahami fitur IAM yang tersedia untuk digunakan dengan AWS WA Tool.

Fitur IAM yang dapat Anda gunakan dengan AWS Well-Architected Tool

Fitur IAM	Dukungan AWS WA Tool
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Peran terkait layanan	Tidak

Untuk mendapatkan gambaran tingkat tinggi tentang cara AWS WA Tool dan layanan AWS lain bekerja dengan sebagian besar fitur IAM, lihat [Layanan AWS yang bekerja dengan IAM](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas AWS WA Tool

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses terhadap apa. Artinya, principal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan 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.

Kebijakan berbasis sumber daya dalam AWS WA Tool

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Principal dapat mencakup akun, pengguna, peran, pengguna terfederasi, atau Layanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk AWS WA Tool

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses terhadap apa. Artinya, principal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan 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 di AWS WA Tool menggunakan prefiks berikut sebelum tindakan: `wellarchitected:`. Misalnya, untuk mengizinkan entitas menentukan beban kerja, administrator harus melampirkan kebijakan yang mengizinkan `wellarchitected:CreateWorkload` tindakan.

Demikian pula, untuk mencegah entitas menghapus beban kerja, administrator dapat melampirkan kebijakan yang menolak tindakan `wellarchitected:DeleteWorkload`. Pernyataan kebijakan harus menyertakan elemen `Action` atau `NotAction`. AWS WA Tool menentukan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk melihat daftar tindakan AWS WA Tool, lihat [Tindakan yang Ditentukan oleh AWS Well-Architected Tool](#) dalam Referensi Otorisasi Layanan.

Sumber daya kebijakan

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses terhadap apa. Artinya, principal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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

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

Untuk melihat daftar jenis sumber daya AWS WA Tool dan ARN-nya, lihat [Sumber daya yang ditentukan oleh AWS Well-Architected Tool](#) dalam Referensi Otorisasi Layanan. Untuk mempelajari dengan tindakan mana Anda dapat menentukan ARN setiap sumber daya, lihat [Tindakan yang ditentukan oleh AWS Well-Architected Tool](#).

Sumber daya beban kerja AWS WA Tool memiliki ARN berikut:

```
arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}
```

Untuk informasi selengkapnya tentang format ARN, lihat [Amazon Resource Name \(ARN\) dan Namespace Layanan AWS](#).

ARN dapat ditemukan di halaman Properti beban kerja untuk beban kerja. Misalnya, untuk menentukan beban kerja tertentu:

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/11112222333344445555666677778888"
```

Untuk menetapkan semua beban kerja milik akun tertentu, gunakan wildcard (*):

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/*"
```

Beberapa tindakan AWS WA Tool, seperti yang digunakan untuk membuat dan menampilkan daftar sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

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

Untuk melihat daftar jenis sumber daya AWS WA Tool dan ARN-nya, lihat [Sumber Daya yang Ditentukan oleh AWS Well-Architected Tool](#) dalam Referensi Otorisasi Layanan. Untuk mempelajari dengan tindakan mana Anda dapat menentukan ARN setiap sumber daya, lihat [Tindakan yang ditentukan oleh AWS Well-Architected Tool](#).

Kunci kondisi kebijakan untuk AWS WA Tool

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses terhadap apa. Artinya, principal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi global AWS, lihat [Kunci konteks kondisi global AWS](#) dalam Panduan Pengguna IAM.

AWS WA Tool mendukung kunci kondisi khusus layanan (`wellarchitected:JiraProjectKey`) dan mendukung penggunaan sebagian kunci kondisi global. Untuk melihat semua kunci kondisi global AWS, lihat [Kunci Konteks Kondisi Global AWS](#) dalam Referensi Otorisasi Layanan.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses terhadap apa. Artinya, principal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama

dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi global AWS, lihat [Kunci konteks kondisi global AWS](#) dalam Panduan Pengguna IAM.

ACL di AWS WA Tool

Mendukung ACL: Tidak

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

Otorisasi berdasarkan tanda AWS WA Tool

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut tanda. Anda dapat melampirkan tanda ke entitas IAM dan sumber daya AWS, lalu merancang kebijakan ABAC untuk mengizinkan operasi ketika tanda principal cocok dengan tanda pada sumber daya.

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

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

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

Menggunakan kredensial sementara dengan AWS WA Tool

Mendukung kredensial sementara: Ya

Kredensial sementara menyediakan akses jangka pendek ke sumber daya AWS dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensial sementara alih-alih menggunakan kunci akses jangka

panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

Izin principal lintas layanan untuk AWS WA Tool

Mendukung sesi akses terusan (FAS): Ya

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

Peran layanan untuk AWS WA Tool

Mendukung peran layanan: Tidak

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

Peran terkait untuk AWS WA Tool

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang tertaut dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

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

Contoh kebijakan berbasis identitas AWS Well-Architected Tool

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya AWS WA Tool. Mereka juga tidak dapat melakukan tugas menggunakan API Konsol Manajemen AWS, AWS CLI, atau AWS. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna atau grup yang memerlukan izin tersebut.

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

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol AWS WA Tool](#)
- [Izinkan para pengguna untuk melihat izin mereka sendiri](#)
- [Memberikan akses penuh ke beban kerja](#)
- [Memberikan akses hanya baca ke beban kerja](#)
- [Mengakses satu beban kerja](#)
- [Menggunakan kunci kondisi khusus layanan untuk Konektor AWS Well-Architected Tool untuk Jira](#)

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan yang dikelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan yang dikelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan ini ada di Akun AWS Anda. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa

semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifik, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Wajibkan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang memerlukan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Menggunakan konsol AWS WA Tool

Untuk mengakses konsol AWS Well-Architected Tool, Anda harus memiliki rangkaian izin minimum. Izin ini harus mengizinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya AWS WA Tool di akun Akun AWS Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa entitas tersebut masih dapat menggunakan konsol AWS WA Tool, lampirkan kebijakan yang dikelola AWS berikut ini ke entitas.

```
WellArchitectedConsoleReadOnlyAccess
```

Untuk memungkinkan kemampuan membuat, mengubah, dan menghapus beban kerja, lampirkan kebijakan terkelola AWS berikut ke entitas:

```
WellArchitectedConsoleFullAccess
```

Untuk informasi selengkapnya, lihat [Menambahkan Izin ke Pengguna](#) dalam Panduan Pengguna IAM.

Anda tidak perlu mengizinkan konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau API AWS. 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 pada konsol atau menggunakan API AWS CLI atau AWS secara programatis.

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

```

Memberikan akses penuh ke beban kerja

Dalam contoh ini, Anda ingin memberi pengguna di Akun AWS Anda akses penuh ke beban kerja Anda. Akses penuh memungkinkan pengguna melakukan semua tindakan di AWS WA Tool. Akses ini diperlukan untuk menentukan beban kerja, menghapus beban kerja, melihat beban kerja, dan memperbarui beban kerja.

JSON

```

{
  "Version":"2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource": "*"
    }
  ]
}

```

Memberikan akses hanya baca ke beban kerja

Dalam contoh ini, Anda ingin memberi pengguna di Akun AWS Anda akses hanya baca ke beban kerja Anda. Akses hanya baca hanya memungkinkan pengguna melihat beban kerja di AWS WA Tool.

JSON

```

{
  "Version":"2012-10-17",
  "Statement" : [
    {

```

```

    "Effect" : "Allow",
    "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*"
    ],
    "Resource": "*"
  }
]
}

```

Mengakses satu beban kerja

Dalam contoh ini, Anda ingin memberi pengguna di Akun AWS Anda akses hanya baca ke salah satu beban kerja Anda, 99999999999955555555555566666666, di Wilayah us-west-2. ID akun Anda adalah 777788889999.

JSON

```

{
  "Version":"2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*"
      ],
      "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555566666666"
    }
  ]
}

```

Menggunakan kunci kondisi khusus layanan untuk Konektor AWS Well-Architected Tool untuk Jira

Contoh ini menunjukkan cara menggunakan kunci kondisi khusus layanan `wellarchitected:JiraProjectKey` untuk mengontrol proyek Jira mana yang dapat ditautkan ke beban kerja di akun Anda.

Hal berikut ini menjelaskan penggunaan yang relevan untuk kunci kondisi:

- **CreateWorkload:** Saat Anda melampirkan `wellarchitected:JiraProjectKey` ke `CreateWorkload`, Anda dapat menentukan proyek Jira kustom mana yang dapat ditautkan ke beban kerja apa pun yang dibuat oleh pengguna. Misalnya, jika pengguna mencoba membuat beban kerja baru dengan proyek ABC, tetapi kebijakan hanya menentukan proyek PQR, tindakan ini akan ditolak.
- **UpdateWorkload:** Saat Anda melampirkan `wellarchitected:JiraProjectKey` ke `UpdateWorkload`, Anda dapat menentukan proyek Jira kustom mana yang dapat ditautkan ke beban kerja ini atau beban kerja apa pun. Misalnya, jika pengguna mencoba memperbarui beban kerja yang ada dengan proyek ABC, tetapi kebijakan menentukan proyek PQR, tindakan ini akan ditolak. Selain itu, jika pengguna memiliki beban kerja yang ditautkan ke proyek PQR dan mencoba memperbarui beban kerja yang akan ditautkan ke proyek ABC, tindakan ini akan ditolak.
- **UpdateGlobalSettings:** Saat Anda melampirkan `wellarchitected:JiraProjectKey` ke `UpdateGlobalSettings`, Anda dapat menentukan proyek Jira kustom mana yang dapat ditautkan ke Akun AWS. Pengaturan tingkat akun melindungi beban kerja di akun Anda yang tidak menimpa pengaturan Jira tingkat akun. Misalnya, jika pengguna memiliki akses `UpdateGlobalSettings`, dia tidak dapat menautkan beban kerja di akun Anda ke proyek apa pun yang tidak ditentukan dalam kebijakan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "wellarchitected:UpdateGlobalSettings",
        "wellarchitected:CreateWorkload"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIfExists": {
          "wellarchitected:JiraProjectKey": ["ABC, PQR"]
        }
      }
    }
  ]
}
```

```
},
{
  "Sid": "VisualEditor1",
  "Effect": "Allow",
  "Action": [
    "wellarchitected:UpdateWorkload"
  ],
  "Resource": "arn:aws:wellarchitected:us-east-1:111122223333:workload/example-  
workload",
  "Condition": {
    "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
  }
}
]
```

Kebijakan yang dikelola AWS untuk AWS Well-Architected Tool

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

Perlu diingat bahwa kebijakan yang dikelola AWS mungkin tidak memberikan izin hak akses paling rendah untuk kasus penggunaan khusus 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 ditetapkan dalam kebijakan yang dikelola AWS. Apabila AWS memperbarui izin yang ditetapkan dalam kebijakan yang dikelola AWS, pembaruan tersebut memengaruhi semua identitas principal (pengguna, grup, dan peran) yang terkait dengan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat Layanan AWS baru diluncurkan atau operasi API baru tersedia untuk layanan yang sudah ada.

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

Kebijakan terkelola AWS: WellArchitectedConsoleFullAccess

Anda dapat melampirkan kebijakan WellArchitectedConsoleFullAccess ke identitas IAM Anda.

Kebijakan ini juga memberikan akses penuh ke AWS Well-Architected Tool.

Detail izin

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "wellarchitected:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan terkelola AWS: WellArchitectedConsoleReadOnlyAccess

Anda dapat melampirkan kebijakan WellArchitectedConsoleReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini memberikan akses hanya baca ke AWS Well-Architected Tool.

Detail izin

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
    }
  ]
}
```

```
        "Resource": "*"
    }
  ]
}
```

Kebijakan terkelola AWS: AWSWellArchitectedOrganizationsServiceRolePolicy

Anda dapat melampirkan kebijakan `AWSWellArchitectedOrganizationsServiceRolePolicy` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif di AWS Organizations yang diperlukan untuk mendukung integrasi AWS Well-Architected Tool dengan Organisasi. Izin ini memungkinkan akun manajemen organisasi mengaktifkan berbagi sumber daya dengan AWS WA Tool.

Detail izin

Kebijakan ini mencakup izin berikut.

- `organizations:ListAWSServiceAccessForOrganization` – Memungkinkan principal memeriksa apakah akses layanan AWS diaktifkan untuk AWS WA Tool.
- `organizations:DescribeAccount` – Memungkinkan principal mengambil informasi tentang akun di organisasi.
- `organizations:DescribeOrganization` – Memungkinkan principal mengambil informasi tentang konfigurasi organisasi.
- `organizations:ListAccounts` – Memungkinkan principal mengambil daftar akun milik suatu organisasi.
- `organizations:ListAccountsForParent` – Memungkinkan principal mengambil daftar akun milik organisasi dari simpul root yang diberikan dalam organisasi.
- `organizations:ListChildren` – Memungkinkan principal mengambil daftar akun dan unit organisasi milik organisasi dari simpul root yang diberikan dalam organisasi.
- `organizations:ListParents` – Memungkinkan principal mengambil daftar orang tua langsung yang ditentukan oleh OU atau akun dalam suatu organisasi.
- `organizations:ListRoots` – Memungkinkan principal mengambil daftar semua simpul root dalam suatu organisasi.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan terkelola AWS: AWSWellArchitectedDiscoveryServiceRolePolicy

Anda dapat melampirkan kebijakan AWSWellArchitectedDiscoveryServiceRolePolicy ke identitas IAM Anda.

Kebijakan ini memungkinkan AWS Well-Architected Tool mengakses layanan dan sumber daya AWS yang berhubungan dengan sumber daya AWS WA Tool.

Detail izin

Kebijakan ini mencakup izin berikut.

- `trustedadvisor:DescribeChecks` – Menampilkan daftar pemeriksaan Trusted Advisor yang tersedia.
- `trustedadvisor:DescribeCheckItems` – Mengambil data pemeriksaan Trusted Advisor, termasuk status dan sumber daya yang ditandai oleh Trusted Advisor.
- `servicecatalog:GetApplication` – Mengambil detail aplikasi AppRegistry.

- `servicecatalog:ListAssociatedResources` – menampilkan daftar sumber daya yang terkait dengan aplikasi AppRegistry.
- `cloudformation:DescribeStacks` – Mendapatkan detail tumpukan CloudFormation.
- `cloudformation:ListStackResources` – Menampilkan daftar sumber daya yang terkait dengan tumpukan CloudFormation.
- `resource-groups:ListGroupResources` – Menampilkan daftar sumber daya dari ResourceGroup.
- `tag:GetResources` – Diperlukan untuk ListGroupResources.
- `servicecatalog>CreateAttributeGroup` – Membuat grup atribut yang dikelola layanan jika diperlukan.
- `servicecatalog:AssociateAttributeGroup` – Mengaitkan grup atribut yang dikelola layanan dengan aplikasi AppRegistry.
- `servicecatalog:UpdateAttributeGroup` – Memperbarui grup atribut yang dikelola layanan.
- `servicecatalog:DisassociateAttributeGroup` – Memisahkan grup atribut yang dikelola layanan dari aplikasi AppRegistry.
- `servicecatalog>DeleteAttributeGroup` – Menghapus grup atribut yang dikelola layanan jika diperlukan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
```

```
"cloudformation:ListStackResources",
"resource-groups:ListGroupResources",
"tag:GetResources"
],
"Resource": [
  "*"
]
},
{
  "Effect": "Allow",
  "Action": [
    "servicelog:ListAssociatedResources",
    "servicelog:GetApplication",
    "servicelog>CreateAttributeGroup"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "servicelog:AssociateAttributeGroup",
    "servicelog:DisassociateAttributeGroup"
  ],
  "Resource": [
    "arn:*:servicelog:*:*:/applications/*",
    "arn:*:servicelog:*:*:/attribute-groups/AWS_WellArchitected-*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "servicelog:UpdateAttributeGroup",
    "servicelog>DeleteAttributeGroup"
  ],
  "Resource": [
    "arn:*:servicelog:*:*:/attribute-groups/AWS_WellArchitected-*"
  ]
}
]
}
```

Pembaruan AWS WA Tool terhadap kebijakan terkelola AWS

Lihat detail tentang pembaruan terhadap kebijakan terkelola AWS untuk AWS WA Tool sejak layanan ini mulai melacak perubahan-perubahan tersebut. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganalah umpan RSS di halaman [Revisi dokumen](#) AWS WA Tool.

Perubahan	Deskripsi	Tanggal
Kebijakan terkelola yang diubah AWS WA Tool	Menambahkan "wellarchitected:Export*" ke WellArchitectedConsoleReadOnlyAccess .	22 Juni 2023
Kebijakan peran layanan yang ditambahkan AWS WA Tool	Menambahkan AWSWellArchitectedDiscoveryServiceRolePolicy untuk memungkinkan AWS Well-Architected Tool mengakses layanan dan sumber daya AWS yang berhubungan dengan sumber daya AWS WA Tool.	3 Mei 2023
Izin yang ditambahkan AWS WA Tool.	Menambahkan tindakan baru untuk memberikan ListAWSServiceAccessForOrganization agar AWS WA Tool dapat memeriksa apakah akses layanan AWS diaktifkan untuk AWS WA Tool.	22 Juli 2022
AWS WA Tool mulai melacak perubahan	AWS WA Tool mulai melacak perubahan untuk kebijakan terkelola AWS.	22 Juli 2022

Pemecahan masalah identitas dan akses AWS Well-Architected Tool

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temukan saat bekerja dengan AWS WA Tool dan IAM.

Topik

- [Saya tidak diotorisasi untuk melakukan tindakan di AWS WA Tool](#)

Saya tidak diotorisasi untuk melakukan tindakan di AWS WA Tool

Jika Konsol Manajemen AWS memberi tahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, Anda harus menghubungi administrator guna mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna IAM *mateojackson* mencoba menggunakan konsol untuk melakukan tindakan `DeleteWorkload`, tetapi tidak memiliki izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
perform: wellarchitected>DeleteWorkload on resource: 11112222333344445555666677778888
```

Dalam hal ini, minta administrator Anda memperbarui kebijakan Anda agar Anda dapat mengakses sumber daya 11112222333344445555666677778888 menggunakan tindakan `wellarchitected>DeleteWorkload`.

Respons insiden di AWS Well-Architected Tool

Respons insiden untuk AWS Well-Architected Tool adalah tanggung jawab AWS. AWS memiliki kebijakan dan program formal terdokumentasi yang mengatur respons insiden.

Masalah operasional AWS dengan dampak luas di-posting di [Service Health Dashboard AWS](#).

Masalah operasional juga di-posting ke akun individu melalui Dasbor AWS Health. Untuk informasi tentang cara menggunakan Dasbor Health, lihat [Panduan Pengguna AWS Health](#).

Validasi kepatuhan untuk AWS Well-Architected Tool

Untuk mempelajari apakah Layanan AWS berada dalam cakupan program kepatuhan tertentu, lihat [Layanan AWS dalam Cakupan Program Kepatuhan](#) dan pilih program kepatuhan yang Anda inginkan. Untuk informasi umum, lihat [Program Kepatuhan AWS](#).

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

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat [Dokumentasi Keamanan AWS](#).

Ketahanan di AWS Well-Architected Tool

Infrastruktur global AWS dibangun di sekitar Region AWS dan Zona Ketersediaan. Region AWS menyediakan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terhubung dengan jaringan yang memiliki latensi rendah, throughput tinggi, dan redundansi tinggi. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Untuk informasi selengkapnya tentang Region AWS dan Zona Ketersediaan, lihat [Infrastruktur Global AWS](#).

Keamanan infrastruktur di AWS Well-Architected Tool

Sebagai layanan terkelola, AWS Well-Architected Tool dilindungi oleh keamanan jaringan global AWS. Lihat informasi tentang layanan keamanan AWS dan cara AWS melindungi infrastruktur di [Keamanan Cloud AWS](#). Untuk mendesain lingkungan AWS Anda dengan menggunakan praktik terbaik bagi keamanan infrastruktur, lihat [Perlindungan Infrastruktur](#) dalam Pilar Keamanan Kerangka Kerja AWS Well-Architected.

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

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

Analisis konfigurasi dan kerentanan dalam AWS Well-Architected Tool

Konfigurasi dan kontrol IT merupakan tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat [model tanggung jawab bersama](#) AWS.

Pencegahan "confused deputy" lintas layanan

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan. Di AWS, peniruan identitas lintas layanan dapat mengakibatkan masalah "confused deputy". Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan principal layanan yang telah diberi akses ke sumber daya di akun Anda.

Kami merekomendasikan penggunaan kunci konteks kondisi global [aws:SourceArn](#) dan [aws:SourceAccount](#) dalam kebijakan sumber daya untuk membatasi izin yang diberikan oleh AWS Well-Architected Tool ke layanan lain untuk mengakses sumber daya. Gunakan `aws:SourceArn` jika Anda ingin hanya satu sumber daya yang akan dikaitkan dengan akses lintas layanan. Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.

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

Jika nilai `aws:SourceArn` tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global tersebut untuk membatasi izin.

Nilai `aws:SourceArn` harus berupa beban kerja atau lensa.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi global `aws:SourceArn` dan `aws:SourceAccount` di AWS WA Tool untuk mencegah masalah "confused deputy".

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfusedDeputyPreventionExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "wellarchitected.amazonaws.com"
      },
      "Action": "wellarchitected:CreateWorkload",
      "Resource": [
        "arn:aws:wellarchitected:us-east-1:111122223333:ResourceName/*"
      ],
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
        },
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

Berbagai sumber daya AWS WA Tool Anda

Untuk berbagi sumber daya yang Anda miliki, lakukan hal berikut:

- [Aktifkan pembagian sumber daya dalam AWS Organizations](#) (opsional)
- [Berbagi beban kerja](#)
- [Berbagi lensa kustom](#)
- [Berbagi profil](#)
- [Berbagi templat tinjauan](#)

Catatan

- Ketika dibagikan, sumber daya akan tersedia untuk digunakan oleh principal di luar Akun AWS yang membuat sumber daya. Berbagi tidak akan mengubah izin apa pun yang berlaku untuk sumber daya di akun yang membuatnya.
- AWS WA Tool adalah layanan Wilayah. Principal yang menerima pembagian Anda dapat mengakses pembagian sumber daya hanya di Region AWS tempat pembuatannya.
- Untuk berbagi sumber daya di Wilayah yang diperkenalkan setelah 20 Maret 2019, Anda dan Akun AWS yang dibagikan harus mengaktifkan Wilayah tersebut di Konsol Manajemen AWS. Untuk informasi lebih lanjut, lihat [Infrastruktur Global AWS](#).

Aktifkan pembagian sumber daya dalam AWS Organizations

Ketika akun Anda dikelola oleh AWS Organizations, Anda dapat memanfaatkannya untuk berbagi sumber daya dengan lebih mudah. Dengan atau tanpa Organizations, pengguna dapat berbagi dengan akun individual. Namun, jika akun Anda berada dalam suatu organisasi, Anda dapat berbagi dengan akun individual, atau dengan semua akun di organisasi atau di OU tanpa harus menghitung setiap akun.

Untuk berbagi sumber daya dalam suatu organisasi, Anda harus terlebih dahulu menggunakan konsol AWS WA Tool atau AWS Command Line Interface (AWS CLI) untuk mengaktifkan pembagian dengan AWS Organizations. Ketika Anda berbagi sumber daya di organisasi Anda, AWS WA Tool tidak mengirim undangan ke principal. Principal di organisasi Anda mendapatkan akses ke sumber daya yang dibagikan tanpa bertukar undangan.

Saat Anda mengaktifkan pembagian sumber daya dalam organisasi Anda, AWS WA Tool membuat peran terkait layanan yang disebut `AWSServiceRoleForWellArchitected`. Peran ini hanya dapat diambil oleh layanan AWS WA Tool, dan memberikan izin kepada AWS WA Tool untuk mengambil informasi tentang organisasinya, dengan menggunakan kebijakan terkelola AWS `AWWellArchitectedOrganizationsServiceRolePolicy`.

Jika Anda sudah tidak perlu berbagi sumber daya dengan seluruh organisasi atau OU Anda, Anda dapat menonaktifkan pembagian sumber daya.

Persyaratan

- Anda dapat melakukan langkah-langkah ini hanya saat masuk sebagai principal di akun manajemen organisasi.
- Organisasi harus mengaktifkan semua fitur. Untuk informasi selengkapnya, lihat [Mengaktifkan semua fitur di organisasi Anda](#) dalam Panduan Pengguna AWS Organizations.

Important

Anda harus mengaktifkan berbagi dengan AWS Organizations menggunakan konsol AWS WA Tool. Ini memastikan bahwa peran terkait layanan `AWSServiceRoleForWellArchitected` dibuat. Jika Anda mengaktifkan akses tepercaya dengan AWS Organizations menggunakan konsol AWS Organizations atau perintah AWS CLI [enable-aws-service-access](#), peran terkait layanan `AWSServiceRoleForWellArchitected` tidak dibuat, dan Anda tidak dapat berbagi sumber daya di dalam organisasi Anda.

Untuk mengaktifkan pembagian sumber daya di dalam organisasi Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.

Anda harus masuk sebagai principal di akun manajemen organisasi.

2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pilih Aktifkan dukungan AWS Organizations.
4. Pilih Simpan pengaturan.

Untuk menonaktifkan pembagian sumber daya di dalam organisasi Anda

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.

Anda harus masuk sebagai principal di akun manajemen organisasi.

2. Pada panel navigasi kiri, pilih Pengaturan.
3. Batalkan pilihan Aktifkan dukungan AWS Organizations.
4. Pilih Simpan pengaturan.

Memberikan tag ke sumber daya AWS WA Tool Anda

Untuk membantu Anda mengelola sumber daya AWS WA Tool, Anda dapat menetapkan metadata Anda sendiri ke setiap sumber daya dalam bentuk tag. Topik ini menjelaskan tentang tag dan menunjukkan kepada Anda cara membuatnya.

Daftar Isi

- [Dasar-dasar tag](#)
- [Memberikan tag ke sumber daya Anda](#)
- [Pembatasan tag](#)
- [Mengelola tag menggunakan konsol](#)
- [Mengelola tag menggunakan API](#)

Dasar-dasar tag

Tag adalah label yang Anda tetapkan ke sumber daya AWS. Setiap tag terdiri atas sebuah kunci dan sebuah nilai opsional, dan Anda menentukan sendiri keduanya.

Tag memungkinkan Anda untuk mengategorikan sumber daya AWS Anda dengan, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Saat Anda memiliki banyak sumber daya dengan jenis yang sama, Anda dapat mengidentifikasi sumber daya tertentu dengan cepat berdasarkan tag yang telah Anda tetapkan. Misalnya, Anda dapat menentukan serangkaian tag untuk layanan-layanan AWS WA Tool Anda sehingga Anda dapat melacak pemilik dan tingkat tumpukan setiap layanan dengan lebih mudah. Kami sarankan Anda merancang serangkaian kunci tag yang konsisten untuk setiap jenis sumber daya.

Selain itu, tag tidak dapat ditetapkan secara otomatis ke sumber daya Anda. Setelah Anda menambahkan tag, Anda dapat mengedit kunci serta nilai tag atau menghapus tag dari sumber daya kapan saja. Jika Anda menghapus sebuah sumber daya, tag apa pun untuk sumber daya tersebut juga ikut dihapus.

Tag tidak memiliki makna semantik pada AWS WA Tool dan diterjemahkan sebagai serangkaian karakter saja. Anda dapat mengatur nilai tag ke string kosong, tetapi Anda tidak dapat menjadikannya tanpa nilai atau null. Jika Anda menambahkan tag yang memiliki kunci yang sama dengan tag yang sudah ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama.

Anda dapat mengelola tag menggunakan Konsol Manajemen AWS, AWS CLI, dan API AWS WA Tool.

Jika menggunakan AWS Identity and Access Management (IAM), Anda dapat mengontrol pengguna mana di Akun AWS Anda yang memiliki izin untuk membuat, mengedit, atau menghapus tag.

Memberikan tag ke sumber daya Anda

Anda dapat memberikan tag ke sumber daya AWS WA Tool baru atau yang sudah ada.

Jika Anda menggunakan konsol AWS WA Tool, Anda dapat menerapkan tag ke sumber daya baru ketika tag tersebut dibuat atau ke sumber daya yang sudah ada kapan saja. Untuk beban kerja yang sudah ada, Anda dapat memberikan tag melalui tab Properti. Untuk lensa kustom, profil, dan templat tinjauan yang sudah ada, Anda dapat memberikan tag melalui tab Ikhtisar.

Jika Anda menggunakan API AWS WA Tool, AWS CLI, atau AWS SDK, Anda dapat menerapkan tag ke sumber daya baru menggunakan parameter `tags` di pada tindakan API yang relevan atau ke sumber daya yang ada menggunakan tindakan API `TagResource`. Untuk informasi lebih lanjut, lihat [TagResource](#).

Selain itu, beberapa tindakan pembuatan sumber daya memungkinkan Anda menentukan tag untuk sumber daya saat sumber daya tersebut dibuat. Jika tag tidak dapat diterapkan selama pembuatan sumber daya, proses pembuatan sumber daya akan gagal. Hal ini memastikan bahwa sumber daya yang ingin Anda beri tag pada saat pembuatan dapat dibuat dengan tag yang ditentukan atau tidak dibuat sama sekali. Jika Anda memberikan tag ke sumber daya pada saat pembuatan, Anda tidak perlu menjalankan skrip pemberian tag khusus setelah pembuatan sumber daya.

Tabel berikut menjelaskan sumber daya AWS WA Tool yang dapat diberi tag, dan sumber daya yang dapat diberi tag saat dibuat.

Dukungan pemberian tag untuk sumber daya AWS WA Tool

Sumber daya	Mendukung tag	Mendukung penyebaran tag	Mendukung pemberian tag saat pembuatan (AWS WA Tool API, AWS CLI, AWS SDK)
Beban kerja AWS WA Tool	Ya	Tidak	Ya

Sumber daya	Mendukung tag	Mendukung penyebaran tag	Mendukung pemberian tag saat pembuatan (AWS WA Tool API, AWS CLI, AWS SDK)
Lensa kustom AWS WA Tool	Ya	Tidak	Ya
Profil AWS WA Tool	Ya	Tidak	Ya
Templat tinjauan AWS WA Tool	Ya	Tidak	Ya

Pembatasan tag

Batasan dasar berikut berlaku untuk tag:

- Jumlah maksimum tag per sumber daya – 50
- Untuk setiap sumber daya, setiap kunci tag harus unik, dan setiap kunci tag hanya dapat memuat satu nilai.
- Panjang kunci maksimum – 128 karakter Unicode dalam UTF-8
- Panjang nilai maksimum – 256 karakter Unicode dalam UTF-8
- Jika skema pemberian tag Anda digunakan di beberapa layanan dan sumber daya AWS, ingatlah bahwa layanan lain mungkin memiliki pembatasan pada karakter yang diizinkan. Karakter yang umumnya boleh digunakan adalah huruf, angka, spasi yang dapat diwakili dalam UTF-8, serta karakter berikut: + - = . _ : / @.
- Kunci dan nilai tag sensitif huruf besar dan kecil.
- Jangan gunakan `aws :`, `AWS :`, atau kombinasi huruf besar atau huruf kecil dari kata tersebut sebagai prefiks untuk kunci atau nilai karena penggunaannya terbatas untuk AWS. Anda tidak dapat mengedit atau menghapus kunci atau nilai tag dengan prefiks ini. Tag dengan prefiks ini tidak termasuk ke dalam cakupan batas tag per sumber daya Anda.

Mengelola tag menggunakan konsol

Dengan menggunakan konsol AWS WA Tool, Anda dapat mengelola tag yang terkait dengan sumber daya baru atau yang sudah ada.

Menambahkan tag ke sumber daya individu pada saat pembuatan

Anda dapat menambahkan tag ke sumber daya AWS WA Tool saat Anda membuatnya.

Menambahkan dan menghapus tag pada sumber daya individu

AWS WA Tool memungkinkan Anda menambah atau menghapus tag yang terkait dengan sumber daya Anda langsung dari tab Properti untuk beban kerja, dan dari tab Ikhtisar untuk lensa kustom, profil, dan templat tinjauan.

Untuk menambahkan atau menghapus tag di beban kerja

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di bilah navigasi, pilih Wilayah yang akan digunakan.
3. Di panel navigasi kiri, pilih Beban kerja.
4. Pilih beban kerja yang akan diubah, lalu pilih Properti.
5. Di bagian Tag, pilih Kelola tag.
6. Tambah atau hapus tag Anda sesuai kebutuhan.
 - Untuk menambahkan tag, pilih Tambahkan tag baru dan edit Kunci dan Nilai.
 - Untuk menghapus sebuah tag, pilih Hapus.
7. Ulangi proses ini untuk setiap tag yang ingin Anda tambah, ubah, atau hapus. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk menambahkan atau menghapus tag di lensa kustom

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di bilah navigasi, pilih Wilayah yang akan digunakan.
3. Di panel navigasi, pilih Lensa kustom.

4. Pilih nama lensa kustom yang akan diubah.
5. Di bagian Tag pada tab Ikhtisar, pilih Kelola tag.
6. Tambah atau hapus tag Anda sesuai kebutuhan.
 - Untuk menambahkan tag, pilih Tambahkan tag baru dan edit Kunci dan Nilai.
 - Untuk menghapus sebuah tag, pilih Hapus.
7. Ulangi proses ini untuk setiap tag yang ingin Anda tambah, ubah, atau hapus. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk menambahkan atau menghapus tag di profil

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di bilah navigasi, pilih Wilayah yang akan digunakan.
3. Di panel navigasi, pilih Profil.
4. Pilih nama profil yang akan diubah.
5. Di bagian Tag pada tab Ikhtisar, pilih Kelola tag.
6. Tambah atau hapus tag Anda sesuai kebutuhan.
 - Untuk menambahkan tag, pilih Tambahkan tag baru dan edit Kunci dan Nilai.
 - Untuk menghapus sebuah tag, pilih Hapus.
7. Ulangi proses ini untuk setiap tag yang ingin Anda tambah, ubah, atau hapus. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk menambahkan atau menghapus tag di templat tinjauan

1. Masuk ke Konsol Manajemen AWS dan buka konsol AWS Well-Architected Tool di <https://console.aws.amazon.com/wellarchitected/>.
2. Di bilah navigasi, pilih Wilayah yang akan digunakan.
3. Di panel navigasi, pilih Templat tinjauan.
4. Pilih nama templat tinjauan yang akan diubah.
5. Di bagian Tag pada tab Ikhtisar, pilih Kelola tag.
6. Tambah atau hapus tag Anda sesuai kebutuhan.

- Untuk menambahkan tag, pilih Tambahkan tag baru dan edit Kunci dan Nilai.
 - Untuk menghapus sebuah tag, pilih Hapus.
7. Ulangi proses ini untuk setiap tag yang ingin Anda tambah, ubah, atau hapus. Pilih Simpan untuk menyimpan perubahan Anda.

Mengelola tag menggunakan API

Gunakan operasi API AWS WA Tool berikut untuk menambahkan, memperbarui, membuat daftar, dan menghapus tag sumber daya Anda.

Dukungan pemberian tag untuk sumber daya AWS WA Tool

Tugas	Tindakan API
Tambahkan atau timpa satu atau beberapa tag.	TagResource
Hapus satu atau beberapa tag.	UntagResource
Membuat daftar tag untuk sumber daya.	ListTagsForResource

Beberapa tindakan pembuatan sumber daya memungkinkan Anda untuk menentukan tag saat membuat sumber daya. Tindakan berikut mendukung pemberian tag saat pembuatan.

Tugas	Tindakan API
Buat beban kerja	CreateWorkload
Impor lensa baru	ImportLens
Membuat profil	CreateProfile
Buat templat tinjauan	CreateReviewTemplate

Mencatat panggilan API AWS WA Tool dengan AWS CloudTrail

AWS Well-Architected Tool terintegrasi dengan AWS CloudTrail, sebuah layanan yang menyediakan catatan tindakan yang dilakukan oleh pengguna, peran, atau layanan AWS di AWS WA Tool. CloudTrail merekam semua panggilan API untuk AWS WA Tool sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari konsol AWS WA Tool dan panggilan kode ke operasi AWS WA Tool API ini. Jika membuat jejak, Anda dapat mengaktifkan pengiriman peristiwa CloudTrail berkelanjutan ke bucket Amazon S3, termasuk peristiwa untuk AWS WA Tool. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru dalam konsol CloudTrail di Riwayat peristiwa. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke AWS WA Tool, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail lainnya.

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

Informasi AWS WA Tool di CloudTrail

CloudTrail diaktifkan di Akun AWS Anda saat Anda membuat akun. Ketika aktivitas terjadi di AWS WA Tool, aktivitas tersebut dicatat dalam peristiwa CloudTrail bersama peristiwa layanan AWS lainnya di Riwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi lebih lanjut, lihat [Melihat Peristiwa dengan Riwayat Peristiwa CloudTrail](#).

Untuk catatan berkelanjutan tentang peristiwa di Akun AWS, termasuk peristiwa untuk AWS WA Tool, buat jejak. Jejak memungkinkan CloudTrail mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Region AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi layanan AWS lainnya untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di log CloudTrail. Untuk informasi selengkapnya, lihat berikut ini:

- [Gambaran Umum untuk Membuat Jejak](#)
- [Layanan dan Integrasi yang Didukung CloudTrail](#)
- [Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima File Log CloudTrail dari Beberapa Wilayah](#) dan [Menerima File log CloudTrail dari Beberapa Akun](#)

Semua tindakan AWS WA Tool dicatat oleh CloudTrail dan didokumentasikan di [Tindakan yang ditentukan oleh AWS Well-Architected Tool](#). Misalnya, panggilan untuk tindakan `CreateWorkload`, `DeleteWorkload`, dan `CreateWorkloadShare` menghasilkan entri di file log CloudTrail.

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

- Baik permintaan tersebut dibuat dengan kredensial pengguna atau pengguna root.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh layanan AWS lainnya.

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

Memahami entri file log AWS WA Tool

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang telah Anda tentukan. File log CloudTrail berisi satu atau beberapa entri log. Peristiwa merepresentasikan satu permintaan dari sumber apa pun dan menyertakan informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. File log CloudTrail tidak merekam panggilan API publik dalam urutan yang teratur, sehingga entri-entri di dalamnya tidak selalu muncul sesuai urutan kronologis kejadian yang sebenarnya.

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

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
    "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
    "accountId": "444455556666",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```

        "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
        "accountId": "444455556666",
        "userName": "well-architected-api-svc-integ-test-read-write"
    },
    "webIdFederationData": {},
    "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-10-14T03:41:39Z"
    }
}
},
"eventTime": "2020-10-14T04:43:13Z",
"eventSource": "wellarchitected.amazonaws.com",
"eventName": "CreateWorkload",
"awsRegion": "us-west-2",
"sourceIPAddress": "198.51.100.178",
"userAgent": "aws-internal/3 aws-sdk-java/1.11.848
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
java/1.8.0_262 vendor/Oracle_Corporation",
"requestParameters": {
    "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
    "Description": "****",
    "AwsRegions": [
        "us-west-2"
    ],
    "ReviewOwner": "****",
    "Environment": "PRODUCTION",
    "Name": "****",
    "Lenses": [
        "wellarchitected",
        "serverless"
    ]
},
"responseElements": {
    "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
    "Id": "8cdcdf7add10b181fdd3f686dacffdac"
},
"requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
"eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "444455556666"

```

```
}
```

EventBridge

AWS Well-Architected Tool mengirim peristiwa ke Amazon EventBridge ketika tindakan diambil pada sumber daya Well-Architected. Anda dapat menggunakan EventBridge dan peristiwa-peristiwa ini untuk menulis aturan-aturan yang mengambil tindakan, seperti yang memberikan notifikasi untuk Anda, ketika ada perubahan sumber daya. Untuk informasi selengkapnya, silakan lihat [Apa yang dimaksud dengan Amazon EventBridge?](#)

Note

Peristiwa diberikan dengan dasar upaya terbaik.

Tindakan berikut menghasilkan peristiwa EventBridge:

- Terkait beban kerja
 - Membuat atau menghapus beban kerja
 - Membuat pencapaian
 - Memperbarui properti beban kerja
 - Membagikan atau berhenti membagikan beban kerja
 - Memperbarui status undangan yang dibagikan
 - Menambah atau menghapus tag
 - Memperbarui jawaban
 - Memperbarui catatan tinjauan
 - Menambahkan atau melepas lensa dari beban kerja
- Terkait lensa
 - Mengimpor atau mengekspor lensa kustom
 - Menerbitkan lensa kustom
 - Menghapus lensa kustom
 - Membagikan atau berhenti membagikan lensa kustom
 - Memperbarui status undangan yang dibagikan
 - Menambahkan atau melepas lensa dari beban kerja

Contoh peristiwa dari AWS WA Tool

Bagian ini mencakup contoh peristiwa dari AWS Well-Architected Tool.

Memperbarui jawaban dalam beban kerja

```
{
  "version":"0",
  "id":"00de336a-83cc-b80b-f0e6-f44c88a96050",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.wellarchitected",
  "account":"123456789012",
  "time":"2022-02-17T08:01:25Z",
  "region":"us-west-2",
  "resources":[],
  "detail":{
    "eventVersion":"1.08",
    "userIdentity":{
      "type":"AssumedRole",
      "principalId":"ARO4JUSXMN5ZR6S7LZNP:sample-user",
      "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
      "accountId":"123456789012",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "sessionContext":{
        "sessionIssuer":{
          "type":"Role",
          "principalId":"ARO4JUSXMN5ZR6S7LZNP",
          "arn":"arn:aws:iam::123456789012:role/Admin",
          "accountId":"123456789012",
          "userName":"Admin"
        },
        "webIdFederationData":{},
        "attributes":{
          "creationDate":"2022-02-17T07:21:54Z",
          "mfaAuthenticated":"false"
        }
      }
    }
  },
  "eventTime":"2022-02-17T08:01:25Z",
  "eventSource":"wellarchitected.amazonaws.com",
  "eventName":"UpdateAnswer",
  "awsRegion":"us-west-2",
```

```

    "sourceIPAddress": "10.246.162.39",
    "userAgent": "aws-internal/3 aws-sdk-java/1.12.127
Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
    "requestParameters": {
      "Status": "Acknowledged",
      "SelectedChoices": "****",
      "ChoiceUpdates": "****",
      "QuestionId": "priorities",
      "WorkloadId": "ee73fda518f9bd4aa804c6252e4e37b0",
      "IsApplicable": true,
      "LensAlias": "wellarchitected",
      "Reason": "NONE",
      "Notes": "****"
    },
    "responseElements": {
      "Answer": "****",
      "LensAlias": "wellarchitected",
      "WorkloadId": "ee73fda518f9bd4aa804c6252e4e37b0"
    },
    "requestID": "7bae1153-26a8-4dc0-9307-68b17b107619",
    "eventID": "8339c258-4ddd-48aa-ab21-3f82ce9d79cd",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
  }
}

```

Menerbitkan lensa kustom

```

{
  "version": "0",
  "id": "4054a34b-60a9-53c1-3146-c1a384dba41b",
  "detail-type": "AWS API Call via CloudTrail",
  "source": "aws.wellarchitected",
  "account": "123456789012",
  "time": "2022-02-17T08:58:34Z",
  "region": "us-west-2",
  "resources": [],

```

```

"detail":{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"AssumedRole",
    "principalId":"ARO0A4JUSXMN5ZR6S7LZNP:example-user",
    "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
    "accountId":"123456789012",
    "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
    "sessionContext":{
      "sessionIssuer":{
        "type":"Role",
        "principalId":"ARO0A4JUSXMN5ZR6S7LZNP",
        "arn":"arn:aws:iam::123456789012:role/Admin",
        "accountId":"123456789012",
        "userName":"Admin"
      },
      "webIdFederationData":{},
      "attributes":{
        "creationDate":"2022-02-17T07:21:54Z",
        "mfaAuthenticated":"false"
      }
    }
  },
  "eventTime":"2022-02-17T08:58:34Z",
  "eventSource":"wellarchitected.amazonaws.com",
  "eventName":"CreateLensVersion",
  "awsRegion":"us-west-2",
  "sourceIPAddress":"10.246.162.39",
  "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
  "requestParameters":{
    "IsMajorVersion":true,
    "LensVersion":"****",
    "ClientRequestToken":"03f46163-e95c-4455-8479-266373aa09c7",
    "LensAlias":"****"
  },
  "responseElements":{
    "LensArn":"arn:aws:wellarchitected:us-
west-2:123456789012:lens/6261deecb9def44f9aecc938ca25d94e",
    "LensVersion":"****"
  },
  "requestID":"167b7051-980d-42ee-9967-0b4b3163e948",
  "eventID":"c7ef2b47-419d-45b7-8982-fbade9b558c7",

```

```
    "readOnly":false,  
    "eventType":"AwsApiCall",  
    "managementEvent":true,  
    "recipientAccountId":"123456789012",  
    "eventCategory":"Management"  
  }  
}
```

Revisi dokumen

Tabel berikut menjelaskan dokumentasi untuk rilis AWS Well-Architected Tool ini.

- Versi API: terbaru
- Pembaruan dokumentasi terkini: 13 Oktober 2025

Perubahan	Deskripsi	Tanggal
Menambahkan bagian Peninjauan Kerangka Kerja Well-Architected (WAFR)	Menambahkan bagian baru dengan panduan untuk melakukan WAFR menggunakan AWS Well-Architected Tool.	13 Oktober 2025
Lensa baru	Rilis ini menambahkan satu lensa baru ke Katalog Lensa.	17 April 2025
Lensa baru dan yang diperbarui	Rilis ini menambahkan satu lensa baru ke Katalog Lensa.	27 Juni 2024
Jira	Rilis ini menambahkan Konektor AWS Well-Architected Tool untuk Jira.	16 April 2024
Lensa baru	Rilis ini menambahkan satu lensa baru ke Katalog Lensa.	26 Maret 2024
Fungsionalitas diperbarui	Rilis ini menambahkan fitur Katalog Lensa ke AWS WA Tool.	26 November 2023
Fungsionalitas diperbarui	Rilis ini menambahkan fitur Templat Tinjauan ke AWS WA Tool.	3 Oktober 2023
Kebijakan terkelola WellArchitectedConsoleReadOnlyAccess diperbarui	Menambahkan "wellarchitected:ExportLens"	22 Juni 2023

	ke <code>WellArchitectedConsoleReadOnlyAccess</code> .	
Fungsionalitas diperbarui	Rilis ini menambahkan fitur Profil ke AWS WA Tool.	13 Juni 2023
Fungsionalitas diperbarui	Rilis ini meningkatkan integrasi AWS Trusted Advisor dan AWS Service Catalog AppRegistry, serta menambahkan <code>AWSWellArchitectedDiscoveryServiceRolePolicy</code> ke kebijakan terkelola AWS.	3 Mei 2023
Pembaruan konten	Halaman Dasbor diperbarui untuk menyertakan detail risiko dan informasi rencana perbaikan. Kemampuan untuk membuat laporan beban kerja terkonsolidasi juga ditambahkan.	30 Maret 2023
Pembaruan konten	Nama kebijakan <code>WellArchitectedConsoleReadOnlyAccess</code> yang dikoreksi.	19 Januari 2023
Memperbarui panduan IAM untuk AWS WA Tool	Memperbarui panduan untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi lebih lanjut, lihat Praktik terbaik keamanan di IAM .	4 Januari 2023
Fungsionalitas diperbarui	Rilis ini menghapus lensa FTR dari alat.	14 Desember 2022

Fungsionalitas diperbarui	Rilis ini menambahkan integrasi AWS Trusted Advisor dan AWS Service Catalog AppRegistry.	7 November 2022
Pembaruan konten	Memperbaiki masalah dalam contoh JSON lensa kustom untuk choices.	29 September 2022
Pembaruan konten	Bagian choices dalam spesifikasi JSON lensa kustom telah diperbarui.	2 Agustus 2022
Fungsionalitas diperbarui	Rilis ini menambahkan perubahan pelacakan untuk kebijakan terkelola AWS-nya dan menambahkan tindakan baru untuk memberikan izin <code>ListAWSServiceAccessForOrganization</code> ke <code>AWSWellArchitectedOrganizationsServiceRolePolicy</code> .	22 Juli 2022
Kemampuan berbagi organisasi ditambahkan	Rilis ini menambahkan kemampuan untuk berbagi beban kerja dan lensa kustom dengan organisasi dan unit organisasi (OU).	30 Juni 2022

Fungsionalitas diperbarui	Rilis ini menambahkan kemampuan untuk menentukan sumber daya tambahan untuk pilihan dalam lensa kustom, untuk melihat pratinjau lensa kustom sebelum memublikasikannya, dan menambahkan tag ke lensa kustom.	21 Juni 2022
Fungsionalitas diperbarui	Rilis ini menambahkan kemampuan untuk mengakses komunitas AWS Well-Architected di AWS re:Post.	31 Mei 2022
Fungsionalitas diperbarui	Rilis ini menambahkan pilar keberlanjutan dan pembaruan kecil ke Tutorial.	31 Maret 2022
Dukungan EventBridge ditambahkan	AWS WA Tool kini memiliki kemampuan untuk mengirim peristiwa ke Amazon EventBridge setiap kali terjadi perubahan pada sumber daya Well-Architected.	3 Maret 2022
Fungsionalitas diperbarui	Praktik terbaik individu I sekarang dapat ditandai sebagai tidak berlaku.	14 Juli 2021
Penandaan sumber daya tersedia	Rilis ini menambahkan kemampuan untuk menambahkan tanda ke beban kerja.	3 Maret 2021

API kini tersedia	Rilis ini menambahkan AWS WA Tool API. Informasi pencatatan AWS CloudTrail ditambahkan.	16 Desember 2020
Fungsionalitas diperbarui	Rilis ini menambahkan lensa FTR dan SaaS ke alat.	3 Desember 2020
Perlindungan data diperbarui	Informasi perlindungan data diperbarui.	5 November 2020
Pembaruan konten	Mengklarifikasi bahwa setelah Anda meningkatkan beban kerja untuk menggunakan lensa baru, Anda tidak dapat kembali ke versi sebelumnya.	8 Juli 2020
Pembaruan konten	Mengklarifikasi kemampuan berbagi di Region AWS yang diperkenalkan setelah 20 Maret 2019.	24 Juni 2020
Fungsionalitas diperbarui	Akses ke pembagian beban kerja segera dihapus saat undangan pembagian beban kerja ditolak. Akses bersama diberikan saat pembagian diterima.	17 Juni 2020
Pembaruan konten	Definisi untuk masalah risiko tinggi (HRI) dan masalah risiko menengah (MRI) ditambahkan.	12 Juni 2020
Pembaruan konten	Bagian tentang cara AWS menggunakan data Anda ditambahkan.	21 Mei 2020

Fungsionalitas diperbarui	Rilis ini menambahkan pemilik tinjauan ke beban kerja.	1 April 2020
Fungsionalitas diperbarui	Rilis ini menambahkan tautan diagram arsitektur ke beban kerja.	10 Maret 2020
Pembaruan konten	Mengklarifikasi bahwa pembagian beban kerja bersifat spesifik per AWS Region.	10 Januari 2020
Fungsionalitas diperbarui	Rilis ini menambahkan kemampuan berbagi beban kerja.	9 Januari 2020
Pembaruan konten	Bagian keamanan diperbarui dengan panduan terbaru.	6 Desember 2019
Fungsionalitas diperbarui	Rilis ini membuat bidang industri bersifat opsional saat menentukan beban kerja.	19 Agustus 2019
Fungsionalitas diperbarui	Rilis ini menambahkan item rencana perbaikan ke laporan beban kerja.	29 Juli 2019
Fungsionalitas diperbarui	Rilis ini menambahkan tindakan DeleteWorkload ke kebijakan.	18 Juli 2019
Pembaruan konten	Isi dalam panduan ini telah diperbarui dengan perbaikan kecil.	19 Juni 2019
Pembaruan konten	Isi dalam panduan ini telah diperbarui dengan perbaikan kecil.	30 Mei 2019

Fungsionalitas diperbarui	Rilis ini mendukung peningkatan versi kerangka kerja yang digunakan untuk tinjauan beban kerja.	1 Mei 2019
Fungsionalitas diperbarui	Rilis ini menambahkan kemampuan untuk menentukan non-Region AWS saat mendefinisikan beban kerja.	14 Februari 2019
AWS Well-Architected Tool Ketersediaan umum	Rilis ini memperkenalkan AWS Well-Architected Tool.	29 November 2018

AWSGlosarium

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