Panduan Pengguna

AWS Well-Architected Tool

AWS Well-Architected Tool: Panduan Pengguna

Table of Contents

Jelajahi dan terapkan teknologi terbaru dan praktik terbaik yang berfokus pada industri dari AWS menggunakan Katalog Lensa.

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

Apakah AWS Well-Architected Tool itu?

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 Toolmembantu Anda sepanjang siklus hidup produk dengan:

- 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 Advisordan AWS Service Catalog AppRegistrymembantu Anda lebih mudah menemukan informasi yang diperlukan untuk menjawab pertanyaan ulasan Well-Architected.

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

Topik

- Kerangka AWS Well-Architected
- Ketentuan

Kerangka AWS Well-Architected

AWSWell-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. Ini menyediakan cara bagi Anda untuk secara konsisten mengukur arsitektur Anda terhadap praktik terbaik dan mengidentifikasi area untuk perbaikan. 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 AWSWell-Architected.

Ketentuan

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 olehAWS, Anda juga dapat membuat dan menggunakan lensa Anda sendiri, atau menggunakan lensa yang telah dibagikan dengan Anda.
- Masalah risiko tinggi (HRI) adalah pilihan arsitektur dan operasional yang AWS telah ditemukan dapat mengakibatkan dampak negatif yang signifikan terhadap bisnis. HRI ini dapat mempengaruhi operasi organisasi, aset, dan individu.
- Masalah risiko menengah (MRI) adalah pilihan arsitektur dan operasional yang mungkin AWS berdampak negatif pada bisnis, tetapi pada tingkat yang lebih rendah daripada HRI.

  Untuk informasi tambahan, lihat Masalah Risiko Tinggi (HRI) dan Masalah Risiko Menengah (MRI).

Memulai dengan AWS Well-Architected Tool

Bagian ini menjelaskan cara memulaiAWS WA Tool.

Topik

Memberikan akses kepada pengguna, grup, atau peran AWS WA Tool

Pada langkah ini, Anda memberikan akses keAWS WA Tool.

Memberikan akses ke AWS WA Tool

1. Untuk memberikan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

   - Pengguna dan grup di AWS IAM Identity Center:

     Buat set izin. Ikuti instruksi di Buat set izin di Panduan Pengguna AWS IAM Identity Center.
   - Pengguna yang dikelola di IAM melalui penyedia identitas:

     Buat peran untuk federasi identitas. Ikuti instruksi dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.
   - Pengguna IAM:
     - Buat peran yang dapat diambil pengguna Anda. Ikuti petunjuk dalam Membuat 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 WellArchitectedConsoleFullAccessterkelola ke set atau peran izin.

Akses penuh memungkinkan prinsipal untuk melakukan semua tindakan diAWS WA Tool. Akses ini diperlukan untuk menentukan beban kerja, menghapus beban kerja, melihat beban kerja, memperbarui beban kerja, berbagi beban kerja, membuat lensa khusus, dan berbagi lensa khusus.

3. Untuk memberikan akses hanya-baca, terapkan kebijakan WellArchitectedConsoleReadOnlyAccessterkelola ke set atau peran izin. Prinsipal dengan peran ini hanya dapat melihat sumber daya.

Untuk informasi lebih lanjut tentang kebijakan ini, lihatAWS kebijakan terkelola untuk AWS Well-Architected Tool.

Mengaktifkan dukungan untuk layanan lain AWS

Mengaktifkan akses Organisasi memungkinkan AWS WA Tool untuk mengumpulkan informasi tentang struktur organisasi Anda untuk berbagi sumber daya dengan lebih mudah (lihat the section called “Aktifkan berbagi sumber daya dalam AWS Organizations” untuk informasi lebih lanjut). Mengaktifkan dukungan Discovery mengumpulkan informasi dari AWS Trusted Advisor, AWS Service Catalog AppRegistry, dan sumber daya terkait (seperti AWS CloudFormation tumpukan dalam koleksi AppRegistry sumber daya) untuk membantu Anda lebih mudah menemukan informasi yang diperlukan untuk menjawab pertanyaan ulasan Well-Architected, dan menyesuaikan pemeriksaan untuk beban kerja. Trusted Advisor

Mengaktifkan dukungan untukAWS Organizations, atau mengaktifkan dukungan Discovery secara otomatis membuat peran terkait layanan untuk akun Anda.

Untuk mengaktifkan dukungan untuk layanan lain yang AWS WA Tool dapat berinteraksi, navigasikan ke Pengaturan.

1. Untuk mengumpulkan informasi dariAWS Organizations, aktifkan Aktifkan AWS Organizations dukungan.
2. Aktifkan dukungan Activate Discovery untuk mengumpulkan informasi dari AWS layanan dan sumber daya 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

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

Setiap kali dukungan Discovery diaktifkan dan AppRegistry dikaitkan dengan beban kerja baru atau yang sudah ada, AWS WA Tool buat 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 Discovery diaktifkan, setiap kali ada perubahan pada beban kerja, grup atribut diperbarui.
- Ketika dukungan Discovery dimatikan atau aplikasi dihapus dari beban kerja, informasi beban kerja dihapus dari. AWS Service Catalog

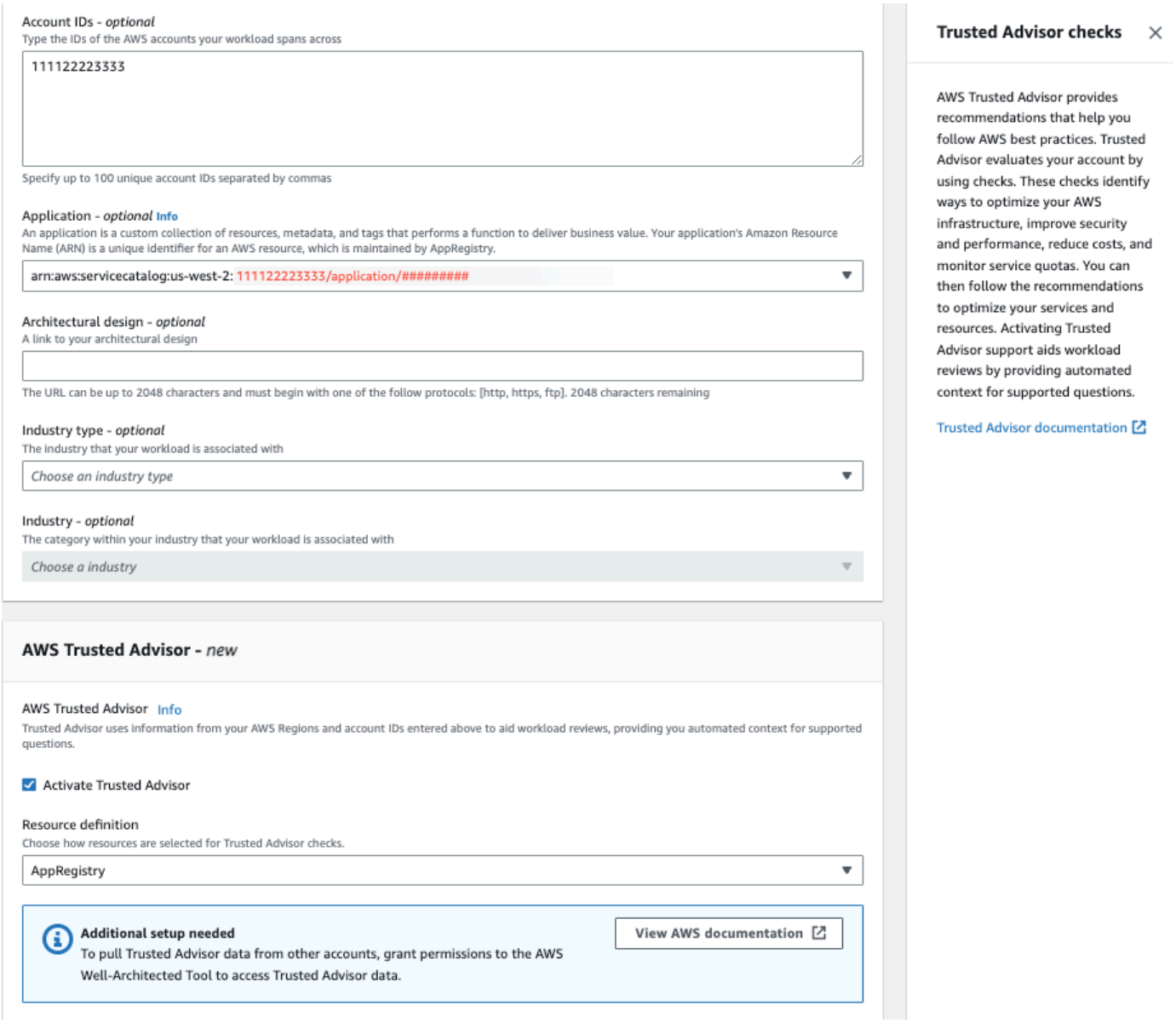
Jika Anda ingin AppRegistry aplikasi menggerakkan data yang diambilTrusted Advisor, tetapkan definisi Sumber Daya beban kerja Anda sebagai AppRegistryatau Semua. Buat peran untuk semua akun yang memiliki sumber daya dalam aplikasi Anda mengikuti pedoman dithe section called “Mengaktifkan Trusted Advisor di IAM”.

Mengaktifkan AWS Trusted Advisor untuk beban kerja

Integrasi dengan AWS Trusted Advisor bersifat opsional, dan dapat diaktifkan berdasarkan per beban kerja untuk pelanggan AWS Business and Enterprise Support. Tidak ada biaya untuk diintegrasikan Trusted AdvisorAWS WA Tool, tetapi untuk detail Trusted Advisor harga, lihat Paket AWS Dukungan.

Untuk mengaktifkan Trusted Advisor untuk beban kerja

1. Untuk mengaktifkanTrusted 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 AWS Trusted Advisorbagian ini, pilih Aktifkan Trusted Advisor.



4. Pemberitahuan bahwa peran layanan IAM akan dibuat ditampilkan saat pertama kali Trusted Advisor diaktifkan untuk beban kerja. Memilih izin Lihat menampilkan izin peran IAM. Anda dapat melihat nama Peran, serta hubungan Izin dan Kepercayaan yang dibuat JSON secara otomatis untuk Anda di IAM. Setelah peran dibuat, untuk mengaktifkan beban kerja berikutnya Trusted Advisor, hanya pemberitahuan untuk Pengaturan tambahan yang diperlukan yang ditampilkan.
5. Di menu tarik-turun Definisi sumber daya, Anda dapat memilih Metadata Beban Kerja,, atau Semua. AppRegistry Pemilihan definisi Resource mendefinisikan data mana yang AWS WA Tool diambil Trusted Advisor untuk memberikan pemeriksaan status dalam tinjauan beban kerja yang memetakan ke praktik terbaik Well-Architected.

Metadata Beban Kerja — beban kerja ditentukan oleh ID akun dan Wilayah AWS ditentukan dalam beban kerja.

AppRegistry— beban kerja ditentukan oleh sumber daya (seperti AWS CloudFormation tumpukan) yang ada dalam AppRegistry aplikasi yang terkait dengan beban kerja.

Semua — beban kerja ditentukan oleh metadata beban kerja dan sumber daya. AppRegistry

6. Pilih Selanjutnya.
7. Terapkan AWSWell-Architected Framework ke beban kerja Anda, dan pilih Tentukan beban kerja. Trusted Advisorpemeriksaan hanya terkait dengan AWS Well-Architected Framework, dan bukan lensa lainnya.

AWS WA ToolSecara berkala mendapatkan data dari Trusted Advisor menggunakan peran yang dibuat di IAM. Peran IAM secara otomatis dibuat untuk pemilik beban kerja. Namun, untuk melihat Trusted Advisor informasi, 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 Trusted Advisor informasi untuk akun itu dan menampilkan kesalahan.

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

Mengaktifkan Trusted Advisor beban kerja di IAM

> **Note**
>
> Pemilik beban kerja harus Aktifkan dukungan Discovery untuk akun mereka sebelum membuat beban Trusted Advisor kerja. Memilih untuk Mengaktifkan dukungan Discovery menciptakan peran yang diperlukan untuk pemilik beban kerja. Gunakan langkah-langkah berikut untuk semua akun terkait lainnya.

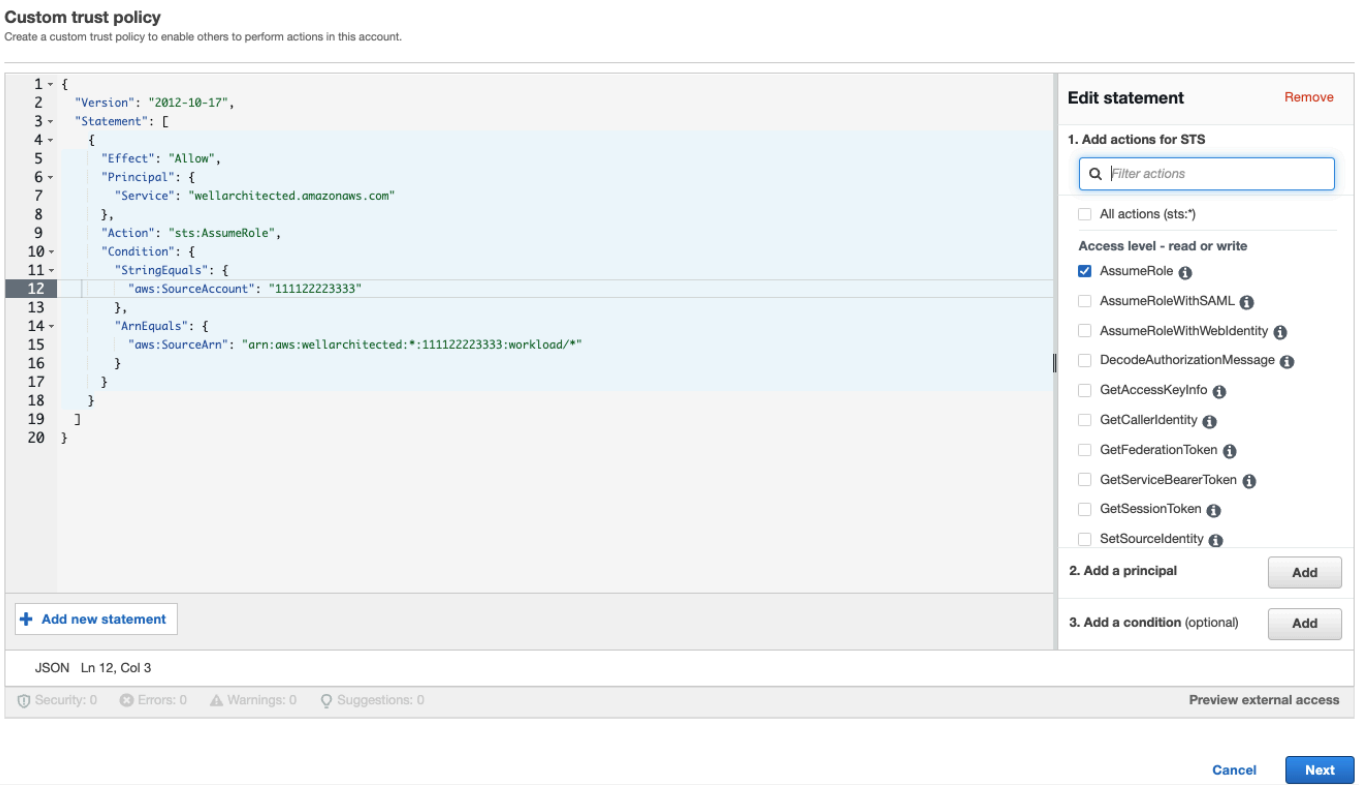
Pemilik akun terkait untuk beban kerja yang telah diaktifkan Trusted Advisor harus membuat peran dalam IAM untuk melihat Trusted Advisor informasi di. AWS WA Tool

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

1. Masuk ke AWS Management Console dan buka konsol IAM pada https://console.aws.amazon.com/iam/.

2. Di panel navigasi konsol IAM, pilih Peran, lalu pilih Buat peran.
3. Di bawah Jenis entitas tepercaya pilih Kebijakan kepercayaan khusus.
4. Salin dan tempel 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.

```
{
  "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:*:WORKLOAD_OWNER_ACCOUNT_ID:workload/*"
        }
      }
    }
  ]
}
```



> **Note**
>
> Blok kondisi `aws:sourceArn` 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 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.

```
{
    "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:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_1",

 "arn:aws:wellarchitected:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_2"
                    ]
                }
            }
        }
    ]
}
```

5. Pada halaman Tambahkan izin, untuk kebijakan Izin pilih Buat kebijakan untuk memberikan AWS WA Tool akses ke data yang dibaca. Trusted Advisor Memilih Buat kebijakan membuka jendela baru.

> **Note**
>
> Selain itu, Anda memiliki opsi untuk melewatkan pembuatan izin selama pembuatan peran dan membuat kebijakan sebaris setelah membuat peran. Pilih Lihat peran dalam pesan pembuatan peran yang berhasil dan pilih Buat kebijakan sebaris dari menu tarik-turun Tambahkan izin di tab Izin.

6. Salin dan tempel 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:Tag.

   Untuk detail tentang format ARN, lihat Amazon Resource Name (ARN) di Panduan Referensi Umum. AWS

```
{
    "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:*:YOUR_ACCOUNT_ID:checks/*"
            ]
        }
    ]
}
```

7. Jika Trusted Advisor diaktifkan untuk beban kerja dan definisi Sumber Daya disetel ke AppRegistryatau Semua, semua akun yang memiliki sumber daya dalam AppRegistry aplikasi yang dilampirkan ke beban kerja harus menambahkan izin berikut ke kebijakan Izin Trusted Advisor peran mereka.

```
{
    "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 tag. Pilih Next: Review (Selanjutnya: 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 harus mendapatkan pesan sukses di bagian atas halaman yang memberi tahu Anda bahwa peran telah dibuat.
12. Untuk melihat peran dan kebijakan izin terkait, di panel navigasi kiri di bawah Manajemen akses, pilih Peran dan cari namanya. `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* Pilih nama peran untuk memverifikasi bahwa hubungan Izin dan Kepercayaan sudah benar.

Menonaktifkan beban Trusted Advisor kerja

Untuk menonaktifkan Trusted Advisor untuk beban kerja

Anda dapat menonaktifkan Trusted Advisor beban kerja apa pun dari AWS WA Tool dengan mengedit beban kerja Anda dan membatalkan pilihan Aktifkan. Trusted Advisor Untuk informasi selengkapnya tentang mengedit beban kerja, lihatthe section called “Mengedit beban kerja”.

Menonaktifkan Trusted Advisor dari AWS WA Tool tidak 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 dinonaktifkanAWS WA Tool, atau berhenti AWS WA Tool mengumpulkan Trusted Advisor data untuk beban kerja.

Untuk menghapus **`WellArchitectedRoleForTrustedAdvisor`** di IAM

1. Masuk ke AWS Management Console dan buka konsol IAM pada 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) di Panduan Pengguna IAM.

Mendefinisikan beban kerja

Langkah selanjutnya adalah mendefinisikan beban kerja.

Untuk menentukan beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Jika ini adalah pertama kalinya Anda menggunakanAWS WA Tool, Anda melihat halaman yang memperkenalkan Anda pada fitur layanan. Di bagian Tentukan beban kerja, pilih Tentukan beban kerja.

   Bergantian, 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 membutuhkan data ini, dan bagaimana data tersebut akan digunakan?
3. Di kotak Nama, masukkan nama untuk beban kerja Anda.

   > **Note**
   >
   > Nama harus antara 3 dan 100 karakter. Setidaknya tiga karakter tidak boleh spasi. Nama beban kerja harus unik. Spasi dan kapitalisasi diabaikan saat memeriksa keunikan.
4. Di kotak Deskripsi, masukkan deskripsi beban kerja. Deskripsi harus antara 3 dan 250 karakter.
5. Di kotak Pemilik tinjau, masukkan nama, alamat email, atau pengenal untuk grup utama atau individu yang memiliki 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:
   - Wilayah AWS— Pilih Wilayah AWS tempat beban kerja Anda berjalan, satu per satu.
   - AWSNon-region — Masukkan nama Wilayah di luar AWS tempat beban kerja Anda berjalan. Anda dapat menentukan hingga lima Wilayah unik, dipisahkan dengan koma.

Gunakan kedua opsi jika sesuai untuk beban kerja Anda.

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

   Jika Trusted Advisor diaktifkan, ID akun apa pun yang ditentukan digunakan untuk mendapatkan data dariTrusted Advisor. Lihat Mengaktifkan beban kerja AWS Trusted Advisor untuk memberikan AWS WA Tool izin untuk mendapatkan Trusted Advisor data atas nama Anda dalam IAM.

9. (Opsional) Di kotak Aplikasi, masukkan ARN aplikasi dari aplikasi yang ingin Anda kaitkan dengan beban kerja ini. AWS Service Catalog AppRegistry Hanya satu ARN yang dapat ditentukan per beban kerja, dan aplikasi serta beban kerja harus berada di Wilayah yang sama.

10. (Opsional) Di kotak desain Arsitektur, masukkan URL untuk desain arsitektur Anda.

11. (Opsional) Di kotak tipe 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 Trusted Advisorbagian ini, untuk mengaktifkan Trusted Advisor pemeriksaan 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” untuk memberikan AWS WA Tool izin untuk mendapatkan Trusted Advisor data atas nama Anda. Pilih dari Metadata Beban Kerja AppRegistry, atau Semua di bawah Definisi sumber daya untuk menentukan sumber daya apa yang AWS WA Tool digunakan untuk menjalankan pemeriksaan. Trusted Advisor

14. (Opsional) Di tag bagian, tambahkan tag apa pun yang ingin Anda kaitkan dengan beban kerja.

    Untuk informasi lebih lanjut tentang tag, lihatMenandai sumber daya AWS WA Tool Anda.

15. Pilih Selanjutnya.

    Jika kotak yang diperlukan kosong atau jika nilai yang ditentukan tidak valid, Anda harus memperbaiki masalah sebelum dapat melanjutkan.

16. (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 Selanjutnya.

17. Pilih lensa yang berlaku untuk beban kerja ini. Hingga 20 lensa dapat ditambahkan ke beban kerja. Untuk deskripsi AWS lensa resmi, lihat Lensa.

Lensa dapat dipilih dari lensa Kustom (lensa yang Anda buat atau yang dibagikan dengan AndaAkun AWS), Katalog Lensa (lensa AWS resmi tersedia untuk semua pengguna), atau keduanya.

> **Note**
>
> Bagian lensa kustom kosong jika Anda belum membuat lensa khusus atau memiliki lensa khusus yang dibagikan dengan Anda.

> **Sanggahan**
>
> Dengan mengakses dan/atau menerapkan lensa khusus yang dibuat oleh AWS pengguna atau akun lain, Anda mengakui bahwa lensa khusus yang dibuat oleh pengguna lain dan dibagikan dengan Anda adalah Konten Pihak Ketiga sebagaimana didefinisikan dalam Perjanjian AWS Pelanggan.

18. Pilih Tentukan beban kerja.

    Jika kotak yang diperlukan kosong atau jika nilai yang ditentukan tidak valid, Anda harus memperbaiki masalah sebelum beban kerja Anda ditentukan.

Mendokumentasikan beban kerja

Setelah beban kerja ditentukan, Anda mendokumentasikan statusnya.

Untuk mendokumentasikan keadaan beban kerja

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

   Jika tidak, di panel navigasi kiri, pilih Beban kerja dan pilih nama beban kerja untuk membuka halaman detail beban kerja. Pilih Lanjutkan meninjau.

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

2. Anda sekarang disajikan dengan pertanyaan pertama. Untuk setiap pertanyaan:

   a. Baca pertanyaan dan tentukan apakah pertanyaan itu 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.
      - Jika tidak, pilih praktik terbaik yang saat ini Anda ikuti dari daftar.

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

      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 dan pilih. Untuk setiap praktik terbaik yang dipilih, Anda dapat memilih alasan secara opsional 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 rincian tambahan tentang praktik terbaik yang dipilih.

   d. Pilih Berikutnya untuk melanjutkan ke pertanyaan berikutnya.

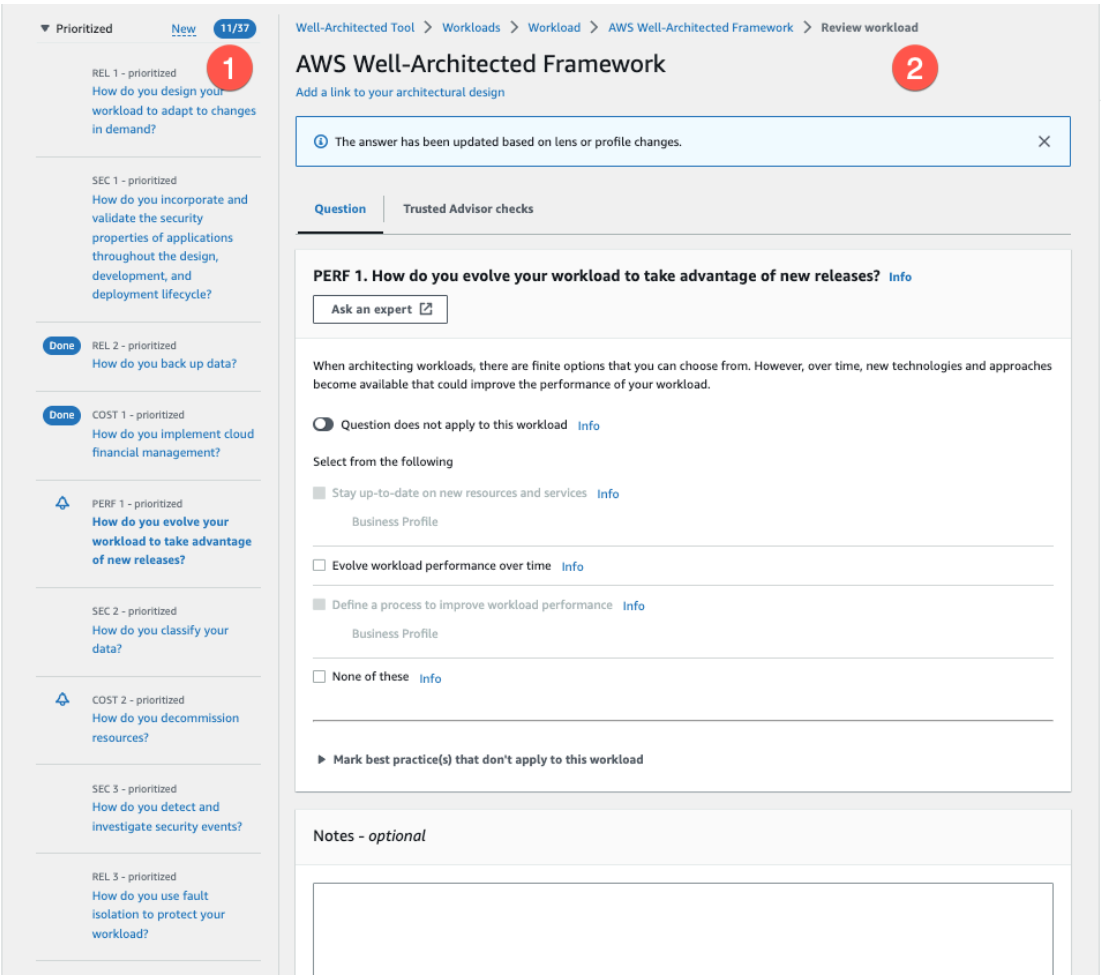
   Ulangi langkah-langkah ini untuk setiap pertanyaan di setiap pilar.

3. Pilih Simpan dan keluar kapan saja untuk menyimpan perubahan dan jeda saat mendokumentasikan beban kerja Anda.

Untuk kembali ke pertanyaan, buka halaman detail beban kerja dan pilih Lanjutkan meninjau.

Tinjau halaman beban kerja

Halaman beban kerja ulasan memiliki tiga panel.



1. 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 dan kemudian memilih pertanyaan yang ingin Anda jawab.

   (Opsional) Jika profil dikaitkan dengan beban kerja Anda, maka AWS WA Tool gunakan informasi di profil untuk menentukan pertanyaan mana dalam tinjauan 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 Minta ahli untuk mengakses komunitas AWS re:Post yang didedikasikan untuk AWS Well-Architected. AWSRe:post adalah pengganti question-and-answer komunitas berbasis topik untuk Forum. AWS

Dengan re:post, Anda dapat menemukan jawaban, menjawab pertanyaan, bergabung dengan grup, mengikuti topik populer, dan memberikan suara pada pertanyaan dan jawaban favorit Anda.

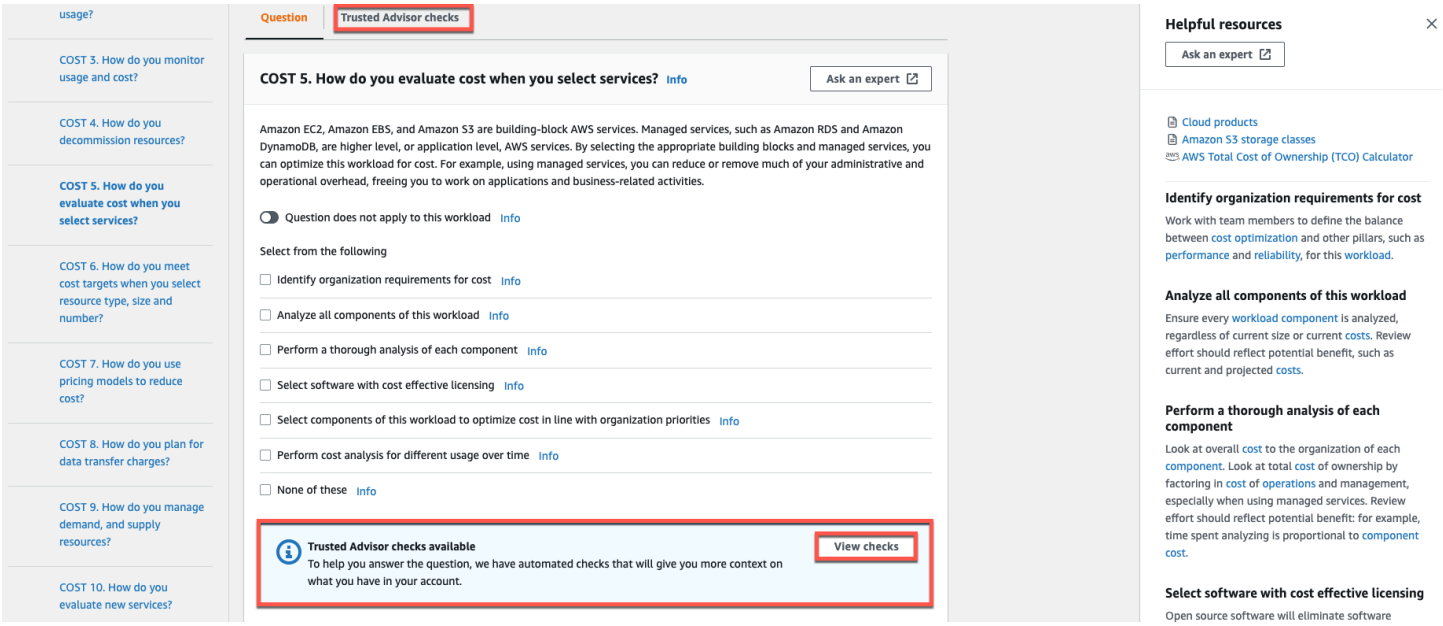
(Opsional) Untuk menandai satu atau beberapa praktik terbaik sebagai tidak berlaku, pilih Tandai praktik terbaik yang tidak berlaku untuk beban kerja ini dan pilih.

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

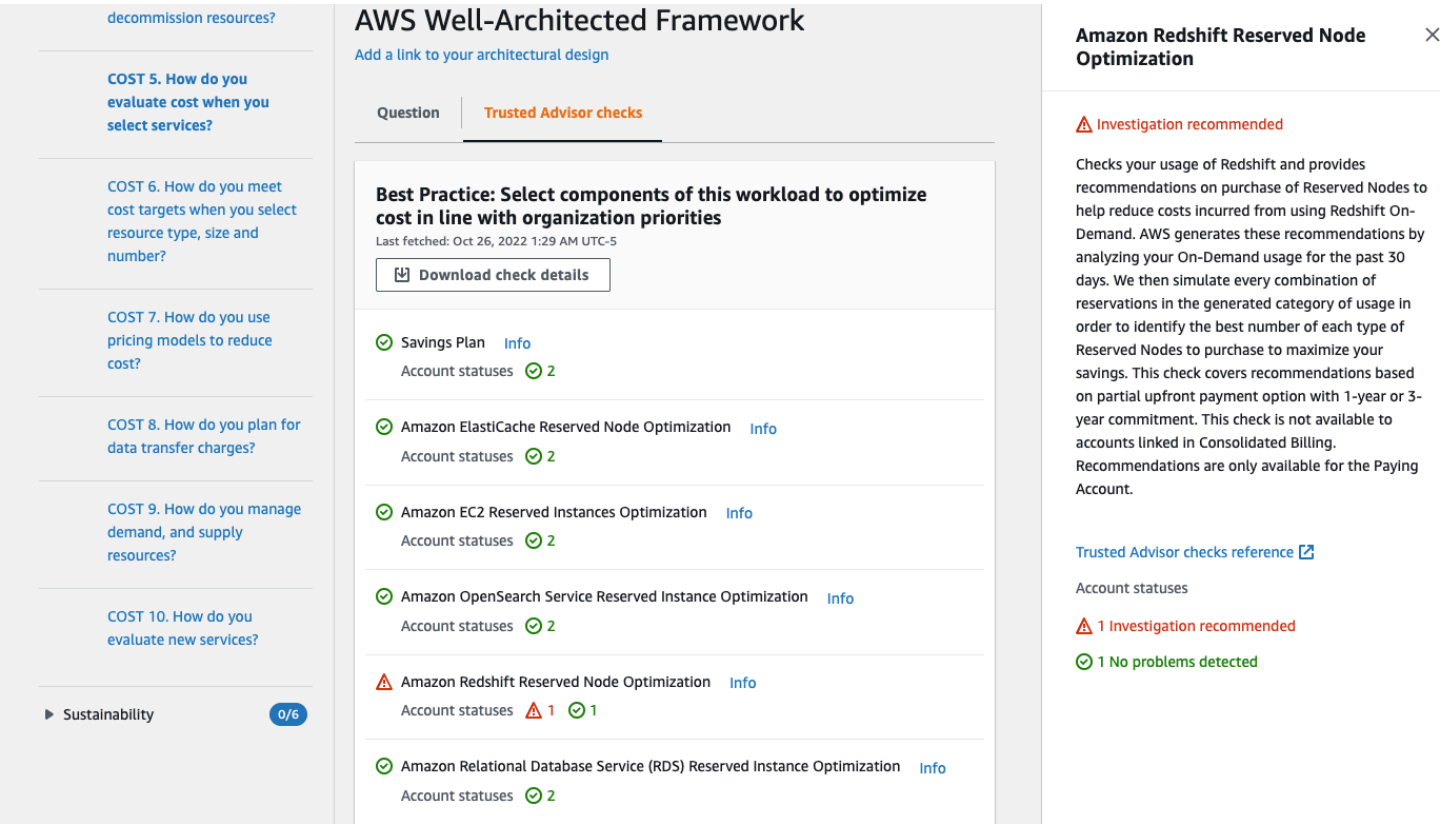
3. Panel bantuan yang tepat menampilkan informasi tambahan dan sumber daya yang bermanfaat. Pilih Minta ahli untuk mengakses komunitas AWS re:Post yang didedikasikan untuk AWS Well-Architected. Di komunitas ini, Anda dapat mengajukan pertanyaan terkait dengan merancang, membangun, menerapkan, dan mengoperasikan beban kerja. AWS

Trusted Advisorcek

Jika Trusted Advisor diaktifkan untuk beban kerja Anda, tab Trusted Advisorcek ditampilkan di sebelah Pertanyaan. Jika ada pemeriksaan yang tersedia untuk praktik terbaik, pemberitahuan bahwa ada Trusted Advisor pemeriksaan yang tersedia ditampilkan mengikuti pemilihan pertanyaan. Memilih Cek tampilan akan membawa Anda ke tab Trusted Advisorcek.



Pada tab Trusted Advisorcek, Anda dapat melihat informasi lebih rinci tentang pemeriksaan praktik terbaik dariTrusted Advisor, melihat tautan ke Trusted Advisor dokumentasi di panel Sumber bantuan, atau Detail pemeriksaan Unduh, yang menyediakan laporan Trusted Advisor pemeriksaan dan status untuk setiap praktik terbaik dalam file CSV.



Kategori cek dari Trusted Advisor ditampilkan sebagai ikon berwarna, dan nomor di samping setiap ikon menunjukkan jumlah akun dalam status itu.

- Tindakan yang direkomendasikan (merah) — Trusted Advisor merekomendasikan tindakan untuk pemeriksaan.
- Investigasi 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 cek yang telah mengecualikan item, seperti sumber daya yang ingin diabaikan oleh cek.

Untuk informasi selengkapnya tentang pemeriksaan yang Trusted Advisor disediakan, lihat Melihat kategori cek di Panduan AWS Support Pengguna.

Memilih tautan Info di samping setiap Trusted Advisor pemeriksaan menampilkan informasi tentang pemeriksaan di panel Sumber bantuan. Untuk informasi selengkapnya, AWS Trusted Advisorlihat referensi di Panduan AWS Support Pengguna.

Menyimpan tonggak sejarah

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

Untuk menyimpan tonggak sejarah

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

> **Note**
>
> Nama harus antara 3 dan 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.

Setelah tonggak sejarah disimpan, Anda tidak dapat mengubah data beban kerja yang ditangkap dalam tonggak tersebut.

Untuk informasi selengkapnya, lihat Tonggak sejarah.

Tutorial

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

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 “Mendefinisikan beban kerja”

Untuk menentukan beban kerja

1. Masuk ke AWS Management Console 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.

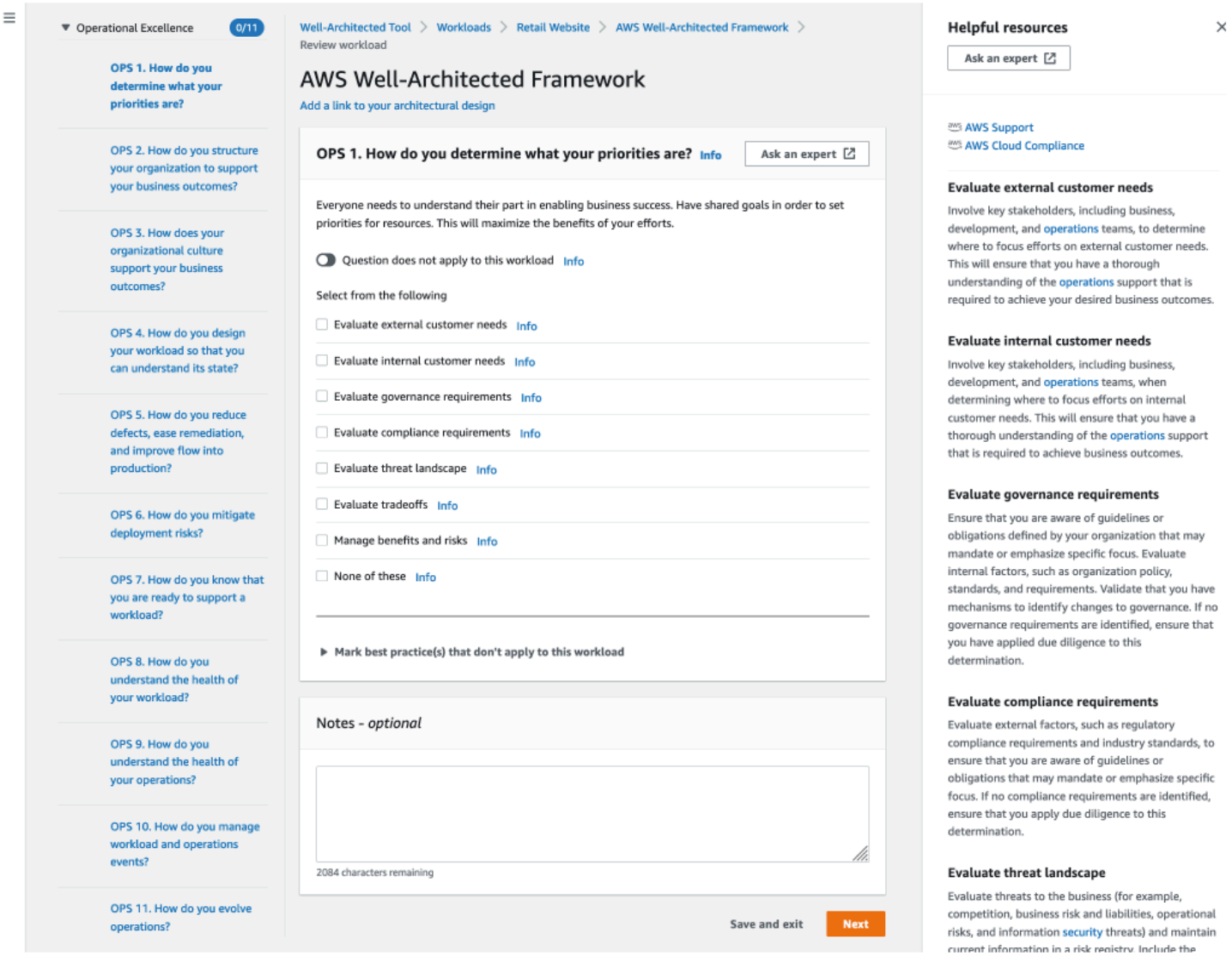
7. Beban kerja kami berjalan pada keduanya AWS dan di pusat data lokal kami:
    a. Pilih Wilayah AWS, dan pilih dua Wilayah di Amerika Utara tempat beban kerja berjalan.
    b. Juga pilih AWSNon-region, dan masukkan nama untuk pusat data lokal.
8. Kotak ID Akun bersifat opsional. Jangan kaitkan apa pun Akun AWS dengan beban kerja ini.
9. Kotak Aplikasi adalah opsional. Jangan masukkan ARN Aplikasi 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. Untuk contoh ini, jangan terapkan tag apa pun ke beban kerja. Pilih Selanjutnya.
14. Langkah Terapkan profil adalah opsional. Jangan menerapkan profil untuk beban kerja ini. Pilih Selanjutnya.
15. 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.
16. 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.

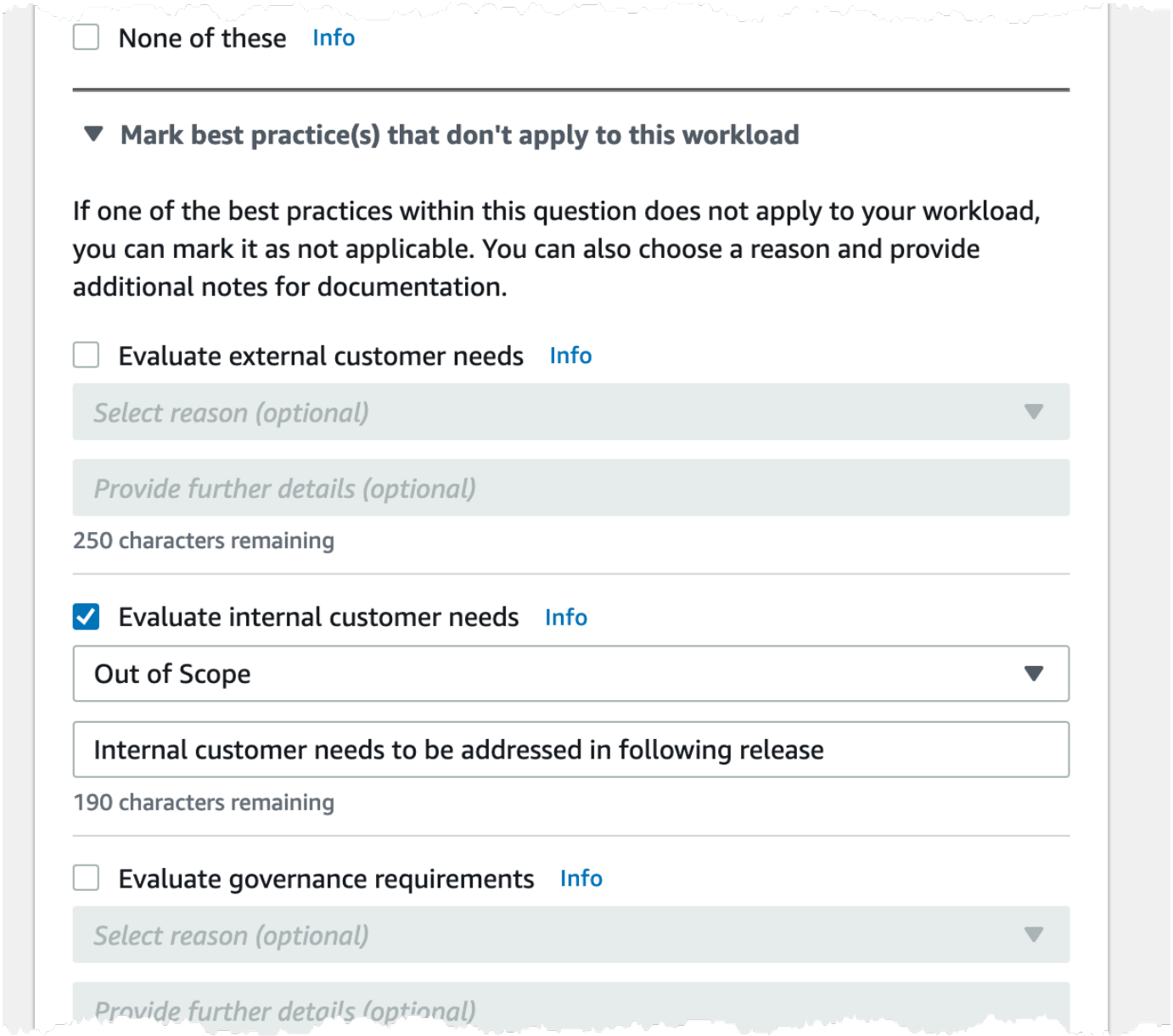
Pilih Minta ahli untuk mengakses komunitas AWS re:Post yang didedikasikan untuk AWS Well-Architected. Di komunitas ini, Anda dapat mengajukan pertanyaan terkait dengan merancang, membangun, menerapkan, dan mengoperasikan beban kerja. AWS



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.



> **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 akan 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 Save (Simpan).
4. Untuk menghasilkan laporan beban kerja, pilih lensa yang diinginkan dan pilih Hasilkan laporan dan file PDF dibuat. File ini berisi status beban kerja, jumlah risiko yang diidentifikasi, dan daftar perbaikan yang disarankan.

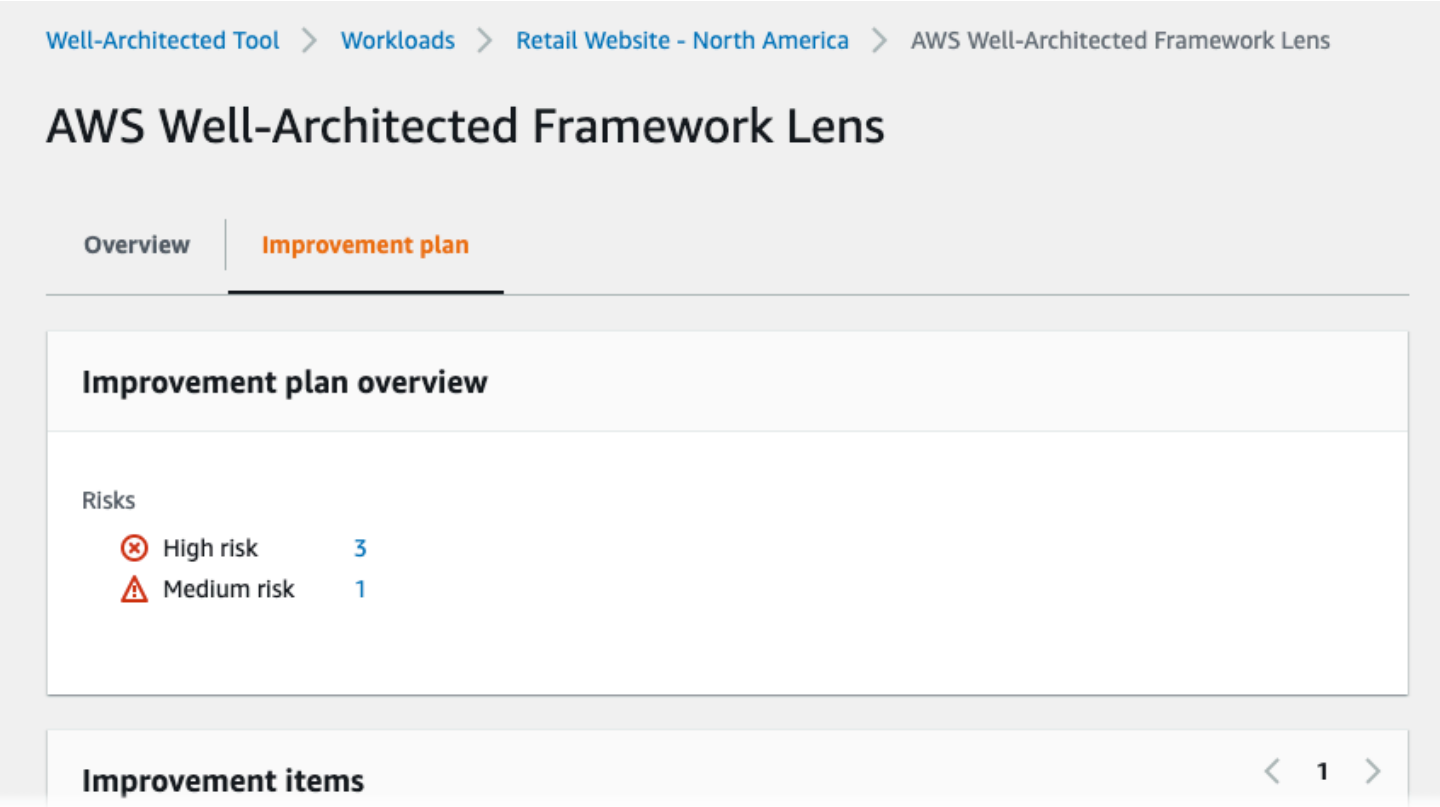
Langkah 3: Tinjau rencana perbaikan

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 AWSWell-Architected Framework dari bagian Lenses pada halaman Ikhtisar.
2. Kemudian pilih Rencana perbaikan.

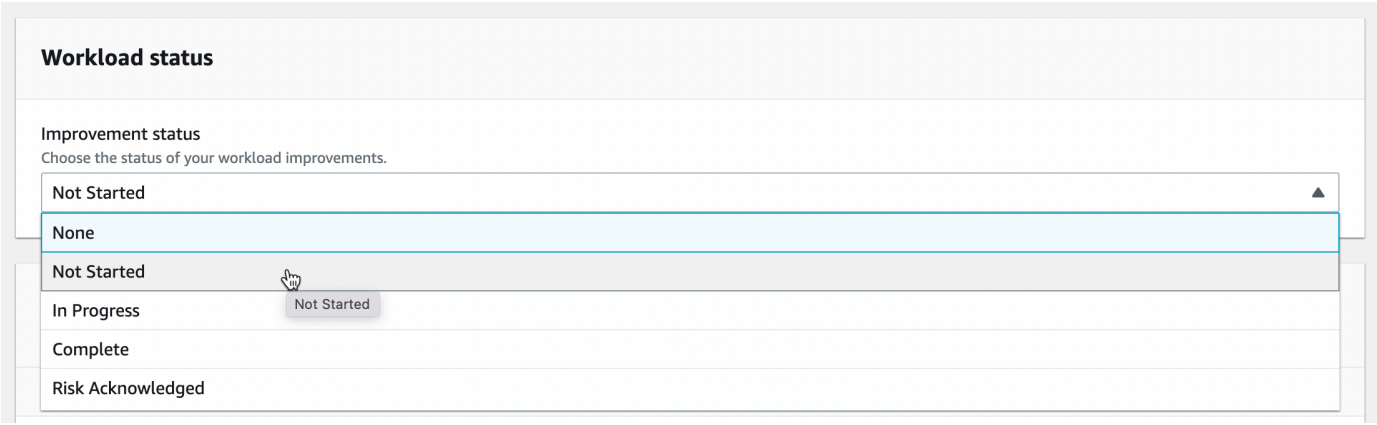
Untuk contoh beban kerja khusus ini, tiga masalah risiko tinggi dan satu masalah risiko menengah diidentifikasi oleh AWS Well-Architected Framework Lens.



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 AWSWell-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.

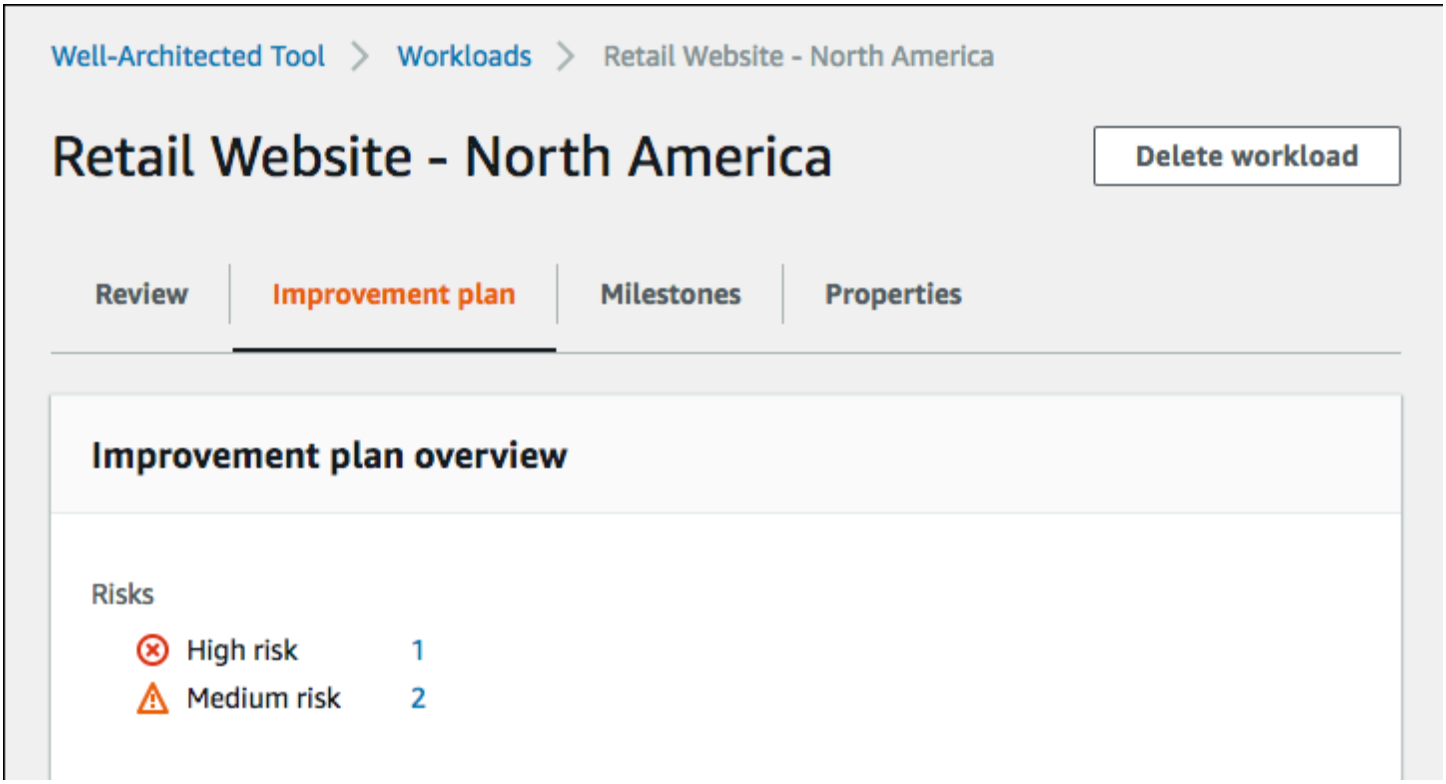
Jika profil dikaitkan dengan beban kerja, hitungan risiko yang diprioritaskan ditampilkan di bagian Ikhtisar rencana perbaikan, dan Anda dapat memfilter daftar item Peningkatan dengan memilih Diprioritaskan berdasarkan profil. Daftar item perbaikan menampilkan label Prioritas.

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 ke 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.



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

Beban kerja

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

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

Halaman Beban Kerja, 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

Akun AWSID yang memiliki beban kerja.

Pertanyaan terjawab

Jumlah pertanyaan yang dijawab.

Risiko tinggi

Jumlah masalah risiko tinggi (HRI) yang diidentifikasi.

Risiko sedang

Jumlah masalah risiko menengah (MRI) yang diidentifikasi.

Status perbaikan

Status perbaikan yang telah Anda tetapkan untuk beban kerja:

- Tidak ada
- Tidak Dimulai
- Sedang Berlangsung
- Lengkap
- Risiko Diakui

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 unit lainAkun AWS, penggunaAWS Organizations, atau organisasi (OU), pilih Lihat detail, lalu Bagikan.
- Untuk menghapus beban kerja dan semua tonggaknya, pilih Hapus. Hanya pemilik beban kerja yang dapat menghapusnya.

> **Warning**
>
> Menghapus beban kerja tidak dapat dibatalkan. Semua data yang terkait dengan beban kerja dihapus.

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

Masalah risiko tinggi (HRI) yang diidentifikasi dalam AWS Well-Architected Tool adalah pilihan arsitektur dan operasional yang AWS telah ditemukan dapat mengakibatkan dampak negatif yang signifikan terhadap bisnis. HRI ini dapat mempengaruhi 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 tanggapan Anda diAWS Well-Architected Tool. Praktik terbaik yang sesuai diterapkan secara luas oleh AWS dan AWS pelanggan. Praktik terbaik ini adalah panduan yang ditentukan oleh AWS Well-Architected Framework dan lensa.

> **Note**
>
> Ini hanya pedoman dan pelanggan harus mengevaluasi dan mengukur dampak apa yang tidak menerapkan praktik terbaik terhadap bisnis mereka. Jika ada alasan teknis atau bisnis tertentu yang mencegah penerapan praktik terbaik pada beban kerja, maka risikonya mungkin lebih rendah dari yang ditunjukkan. AWSmenyarankan agar pelanggan mendokumentasikan alasan-alasan ini, dan bagaimana pengaruhnya terhadap praktik terbaik, dalam catatan beban kerja. Untuk semua HRI dan MRI yang diidentifikasi, AWS

menyarankan pelanggan menerapkan praktik terbaik sebagaimana didefinisikan dalam. AWS Well-Architected Tool Jika praktik terbaik diterapkan, tunjukkan bahwa masalah telah diselesaikan dengan menandai praktik terbaik sebagaimana terpenuhi diAWS Well-Architected Tool. Jika pelanggan memilih untuk tidak menerapkan praktik terbaik, AWS menyarankan agar mereka mendokumentasikan persetujuan tingkat bisnis yang berlaku dan alasan untuk tidak menerapkannya.

Mendefinisikan beban kerja

Ada dua cara untuk menentukan beban kerja. Pada halaman Workloads di AWS WA Tool Anda dapat menentukan beban kerja tanpa template. Atau, pada halaman Templat ulasan, Anda dapat menggunakan templat ulasan yang ada atau membuat templat baru untuk menentukan beban kerja.

Untuk menentukan beban kerja dari halaman Beban Kerja

1. Pilih Beban kerja di panel navigasi kiri.
2. Pilih dropdown Tentukan beban kerja.
3. Pilih Tentukan beban kerja. Atau, jika Anda telah membuat template ulasan dan ingin menentukan beban kerja darinya, pilih Tentukan dari templat ulasan.
4. Ikuti petunjuk the section called “Mendefinisikan beban kerja” untuk menentukan properti beban kerja, atau (opsional) menerapkan profil dan lensa.

Untuk menentukan beban kerja dari halaman Template Review

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

Melihat beban kerja

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

Untuk melihat beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 dan pilih Lihat detail.

Halaman detail beban kerja ditampilkan.

> **Note**
>
> Bidang wajib, Pemilik ulasan, telah ditambahkan untuk memungkinkan Anda mengidentifikasi orang atau grup utama yang bertanggung jawab atas proses peninjauan dengan mudah. Saat pertama kali Anda melihat beban kerja yang ditentukan sebelum bidang ini ditambahkan, Anda akan diberi tahu tentang perubahan ini. Pilih Edit untuk menyetel bidang Pemilik ulasan dan tidak diperlukan tindakan lebih lanjut.
> Pilih Akui untuk menunda pengaturan bidang Pemilik ulasan. Selama 60 hari ke depan, spanduk ditampilkan untuk mengingatkan Anda bahwa bidang tersebut kosong. Untuk menghapus spanduk, edit beban kerja Anda dan tentukan pemilik Tinjauan.
> Jika Anda tidak mengatur bidang pada tanggal yang ditentukan, akses Anda ke beban kerja dibatasi. Anda dapat terus melihat beban kerja dan menghapusnya, tetapi Anda tidak dapat mengeditnya, kecuali untuk menyetel bidang Pemilik Tinjauan. Akses bersama ke beban kerja tidak terpengaruh saat akses Anda terbatas.

Mengedit beban kerja

Anda dapat mengedit detail beban kerja yang Anda miliki.

Untuk mengedit beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di panel navigasi kiri, pilih Beban kerja.

3. Pilih beban kerja yang ingin Anda edit dan pilih Edit.
4. Buat perubahan Anda pada beban kerja.

   Untuk deskripsi masing-masing bidang, lihatMendefinisikan beban kerja.

   > **Note**
   >
   > Saat memperbarui beban kerja yang ada, Anda dapat Aktifkan Trusted Advisor, yang secara otomatis membuat peran IAM untuk pemilik beban kerja. Pemilik akun terkait untuk beban kerja dengan kebutuhan yang Trusted Advisor diaktifkan untuk membuat peran dalam IAM. Untuk detailnya, lihat the section called “Mengaktifkan Trusted Advisor di IAM”.

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

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

Berbagi beban kerja

Anda dapat berbagi beban kerja yang Anda miliki dengan pengguna lainAkun AWS, organisasi, dan unit organisasi (OU) dalam hal yang samaWilayah AWS.

> **Note**
>
> Anda hanya dapat berbagi beban kerja dalam hal yang samaWilayah AWS.
> Saat berbagi beban kerja dengan yang lainAkun AWS, jika penerima tidak memiliki `wellarchitected:UpdateShareInvitation` izin, mereka tidak dapat menerima undangan berbagi. Lihat the section called “Menyediakan akses ke AWS WA Tool” contoh kebijakan izin.

Untuk berbagi beban kerja dengan orang lain Akun AWS dan pengguna

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 dan pilih Lihat detail.

4. Pilih Saham. Kemudian pilih Buat dan Buat berbagi ke pengguna atau akun untuk membuat undangan beban kerja.
5. Masukkan Akun AWS ID 12 digit atau ARN pengguna yang ingin Anda bagikan beban kerja.
6. Pilih izin yang ingin Anda berikan.

   Baca-Saja

   Menyediakan akses read-only 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 yang ditentukan Akun AWS atau pengguna.

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

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

> **Important**
>
> Sebelum berbagi beban kerja dengan organisasi atau unit organisasi (OU), Anda harus mengaktifkan AWS Organizations akses.

Untuk berbagi beban kerja dengan organisasi atau OU Anda

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 dan pilih Lihat detail.

4. Pilih Saham. Kemudian pilih Create and Create shares to Organizations.
5. Pada halaman Buat berbagi beban kerja, pilih apakah akan memberikan izin ke seluruh organisasi, atau ke satu atau beberapa OU.
6. Pilih izin yang ingin Anda berikan.

   Baca-Saja

   Menyediakan akses read-only 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 siapa yang telah berbagi akses ke beban kerja, pilih Berbagi dari Detail beban kerja halaman.

Untuk mencegah entitas berbagi beban kerja, lampirkan kebijakan yang menolak tindakan. `wellarchitected:CreateWorkloadShare`

Anda juga dapat berbagi lensa khusus yang Anda miliki dengan orang lainAkun AWS, pengguna, organisasi Anda, dan OU dalam hal yang samaWilayah AWS. Untuk detailnya, lihatBerbagi lensa kustom.

Berbagi pertimbangan

Beban kerja dapat dibagi dengan hingga 20 pengguna Akun AWS dan berbeda. Beban kerja hanya dapat dibagikan dengan akun dan pengguna yang Wilayah AWS sama dengan beban kerja.

Untuk berbagi beban kerja di Wilayah yang diperkenalkan setelah 20 Maret 2019, Anda dan yang dibagikan Akun AWS harus mengaktifkan Wilayah diAWS Management Console. Untuk informasi lebih lanjut, lihat Infrastruktur AWS Global.

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

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

Sebelum berbagi beban kerja dengan organisasi atau satu atau lebih unit organisasi (OU), Anda harus mengaktifkan AWS Organizations akses.

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

Untuk mengaktifkan AWS Organizations berbagi

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

Menghapus akses bersama

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 AWS Management Console dan buka AWS Well-Architected Tool konsol 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 dan pilih Lihat detail.
4. Pilih Saham.
5. Pilih undangan beban kerja yang akan dihapus dan pilih Hapus.
6. Pilih Hapus untuk mengonfirmasi.

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

Memodifikasi akses bersama

Anda dapat mengubah undangan beban kerja yang tertunda atau diterima.

Untuk mengubah akses bersama ke beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 dan pilih Lihat detail.
4. Pilih Saham.
5. Pilih undangan beban kerja untuk dimodifikasi dan pilih Edit.
6. Pilih izin baru yang ingin Anda berikan kepada Akun AWS atau pengguna.

   Baca-Saja

   Menyediakan akses read-only ke beban kerja.

   Kontributor

   Menyediakan akses pembaruan ke jawaban dan catatannya, dan akses hanya-baca ke sisa beban kerja.
7. Pilih Save (Simpan).

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

Menerima dan menolak undangan beban kerja

Undangan beban kerja adalah permintaan untuk berbagi beban kerja yang dimiliki oleh orang lain. Akun AWS 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 tujuh hari untuk menerima undangan beban kerja. Jika Anda tidak menerima undangan dalam waktu tujuh hari, itu akan kedaluwarsa secara otomatis.

> **Note**
>
> Beban kerja hanya dapat dibagi dalam hal yang samaWilayah AWS.

Untuk menerima atau menolak undangan beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di panel navigasi kiri, pilih Undangan beban kerja.
3. Pilih undangan beban kerja untuk menerima atau menolak.
   - Untuk menerima undangan beban kerja, pilih Terima.

     Beban kerja ditambahkan ke halaman Beban Kerja dan Dasbor.
   - Untuk menolak undangan beban kerja, pilih Tolak.

     Undangan beban kerja dihapus dari daftar.

Untuk menolak akses bersama setelah undangan beban kerja diterima, pilih Tolak berbagi dari Detail beban kerja halaman untuk beban kerja.

Menghapus beban kerja

Anda dapat menghapus beban kerja saat tidak lagi diperlukan. Menghapus beban kerja akan menghapus semua data yang terkait dengan beban kerja termasuk tonggak sejarah dan undangan berbagi beban kerja. Hanya pemilik beban kerja yang dapat menghapusnya.

> **Warning**
>
> Menghapus beban kerja tidak dapat dibatalkan. Semua data yang terkait dengan beban kerja dihapus secara permanen.

Untuk menghapus beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di panel navigasi kiri, pilih Beban kerja.
3. Pilih beban kerja yang ingin Anda hapus dan pilih Hapus.
4. Di jendela Hapus, pilih Hapus untuk mengonfirmasi penghapusan beban kerja dan tonggaknya.

Untuk mencegah entitas menghapus beban kerja, lampirkan kebijakan yang menolak `wellarchitected:DeleteWorkload` tindakan.

Menghasilkan laporan beban kerja

Anda dapat membuat laporan beban kerja untuk lensa. Laporan ini berisi tanggapan Anda terhadap pertanyaan beban kerja, catatan Anda, dan jumlah risiko tinggi dan menengah saat ini yang diidentifikasi. Jika sebuah pertanyaan memiliki satu atau lebih risiko yang diidentifikasi, rencana perbaikan untuk pertanyaan itu mencantumkan tindakan yang harus diambil untuk mengurangi risiko tersebut.

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

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

Untuk menghasilkan laporan beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 dan pilih Hasilkan laporan.

   Laporan dibuat dan Anda dapat mengunduh atau melihatnya.

Detail beban kerja

Halaman detail beban kerja memberikan informasi tentang beban kerja Anda termasuk tonggak pencapaian, rencana peningkatan, dan pembagian beban kerja apa pun. Gunakan tab di bagian atas halaman untuk menavigasi ke bagian detail yang berbeda.

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

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

Topik

Tab Ikhtisar

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

Jika Anda belum menyelesaikan semua pertanyaan, spanduk muncul untuk mengingatkan Anda untuk memulai atau melanjutkan mendokumentasikan beban kerja Anda.

Bagian Ikhtisar beban kerja menunjukkan keadaan keseluruhan beban kerja saat ini dan catatan Beban Kerja apa pun yang telah Anda masukkan. Pilih Edit untuk memperbarui status atau catatan.

Untuk menangkap status beban kerja saat ini, pilih Simpan tonggak sejarah. Tonggak sejarah tidak dapat diubah dan tidak dapat diubah setelah disimpan.

Untuk terus mendokumentasikan keadaan beban kerja, pilih Mulai meninjau dan pilih lensa yang diinginkan.

Tab tonggak sejarah

Untuk menampilkan tonggak untuk beban kerja Anda, pilih tab Milestones.

Setelah Anda memilih tonggak sejarah, pilih Buat laporan untuk membuat laporan beban kerja yang terkait dengan tonggak sejarah. Laporan tersebut berisi tanggapan terhadap pertanyaan beban kerja, catatan Anda, dan jumlah risiko tinggi dan menengah dalam beban kerja pada saat tonggak sejarah disimpan.

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

- Memilih nama tonggak sejarah.
- Memilih tonggak sejarah dan memilih Lihat tonggak sejarah.

Tab properti

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

Untuk deskripsi properti, lihatMendefinisikan beban kerja.

Tab Berbagi

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

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

Utama

Akun AWSID 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 itu diterima.

- Ditolak

  Undangan itu ditolak.
- Kadaluarsa

  Undangan itu tidak diterima atau ditolak dalam waktu tujuh hari.

Izin

Izin yang diberikan kepada Akun AWS atau pengguna.

- Baca-Saja

  Kepala sekolah memiliki akses read-only ke beban kerja.
- Kontributor

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

Detail izin

Deskripsi terperinci tentang izin.

Untuk berbagi beban kerja dengan pengguna lain Akun AWS atau pengguna yang samaWilayah AWS, pilih Buat. Beban kerja dapat dibagi dengan hingga 20 pengguna Akun AWS dan berbeda.

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

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

Lensa

Lensa menyediakan cara bagi Anda untuk secara konsisten mengukur arsitektur Anda terhadap praktik terbaik dan mengidentifikasi area untuk perbaikan. AWS Well-Architected Framework Lens secara otomatis diterapkan ketika beban kerja ditentukan.

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

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

- Katalog Lensa: Lensa resmi yang dibuat dan dipelihara oleh AWS. Katalog Lensa tersedia untuk semua pengguna dan tidak memerlukan instalasi tambahan untuk digunakan.
- Lensa khusus: Lensa yang ditentukan pengguna yang bukan konten AWS resmi. Anda dapat membuat lensa khusus dengan pilar, pertanyaan, praktik terbaik, dan rencana peningkatan Anda sendiri, serta berbagi lensa khusus dengan yang lain Akun AWS.

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

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

Menambahkan lensa ke beban kerja

Untuk menambahkan lensa ke beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 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 AWS lensa, kunjungi AWS Well-Architected Lenses. Perhatikan bahwa tidak setiap whitepaper lensa disediakan sebagai lensa dalam katalog lensa.

> **Sanggahan**
>
> Dengan mengakses dan/atau menerapkan lensa khusus yang dibuat oleh AWS pengguna atau akun lain, Anda mengakui bahwa lensa khusus yang dibuat oleh pengguna lain dan dibagikan dengan Anda adalah Konten Pihak Ketiga sebagaimana didefinisikan dalam Perjanjian AWS Pelanggan.

Melepaskan lensa dari beban kerja

Untuk menghapus lensa dari beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 Anda hapus 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.

Detail lensa

Untuk melihat detail tentang lensa, pilih lensa.

Tab Ikhtisar

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

Tab Berbagi

Untuk lensa kustom, tab Shares menyediakan daftar prinsip IAM yang telah dibagikan lensa.

Lensa kustom

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

Anda dapat menyesuaikan pertanyaan dalam lensa khusus 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 kemajuan dari waktu ke waktu dengan membuat tonggak sejarah, dan memberikan status berkala dengan menghasilkan laporan.

Topik

Melihat lensa khusus

Anda dapat melihat detail lensa khusus yang Anda miliki dan lensa khusus yang telah dibagikan dengan Anda.

Untuk melihat lensa

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 khusus atau memiliki lensa khusus yang dibagikan dengan Anda.

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

Detail lensaHalaman ditampilkan.

Halaman lensa Kustom memiliki bidang-bidang berikut:

Nama

Nama lensa.

Pemilik

Akun AWS ID yang memiliki lensa kustom.

Status

Status PUBLISHED berarti bahwa lensa kustom telah diterbitkan dan dapat diterapkan pada beban kerja atau dibagikan dengan yang lain Akun AWS.

Status DRAFT berarti bahwa lensa kustom telah dibuat tetapi belum dipublikasikan. Lensa khusus 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 khusus

Untuk membuat lensa kustom

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

   Lihat Spesifikasi format lensa untuk detailnya. Lensa khusus tidak boleh melebihi 500 KB.
6. Pilih Pilih file untuk memilih file JSON Anda.
7. (Opsional) Di bagian Tag, tambahkan tag apa pun yang ingin Anda kaitkan dengan lensa khusus.
8. Pilih Kirim & Pratinjau untuk melihat pratinjau lensa kustom, atau Kirim untuk mengirimkan lensa khusus tanpa melihat pratinjau.

   Jika Anda memilih untuk Kirim & Pratinjau lensa kustom Anda, Anda dapat memilih Berikutnya untuk menavigasi melalui pratinjau lensa, atau pilih Exit Preview 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, itu dalam status DRAFT. Anda harus mempublikasikan lensa sebelum dapat diterapkan ke beban kerja atau dibagikan dengan yang lain Akun AWS.

Anda dapat membuat hingga 15 lensa khusus dalam format Akun AWS.

> **Sanggahan**
>
> Jangan menyertakan atau mengumpulkan informasi identitas pribadi (PII) pengguna akhir atau individu lain yang dapat diidentifikasi di dalam atau melalui lensa khusus Anda. Jika lensa kustom Anda atau yang dibagikan dengan 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.

Mempratinjau lensa khusus

Untuk melihat pratinjau lensa kustom

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Hanya lensa dalam status DRAFT yang dapat dipratinjau. Pilih lensa kustom DRAFT yang diinginkan dan pilih Pengalaman pratinjau.
4. Pilih Berikutnya untuk menavigasi melalui pratinjau lensa.
5. (Opsional) Anda dapat meninjau rencana Peningkatan Anda dengan memilih praktik terbaik dalam setiap pertanyaan di pratinjau, dan memilih Pembaruan berdasarkan jawaban untuk menguji logika risiko Anda. Jika ada perubahan yang diperlukan, Anda dapat memperbarui Aturan Risiko di template JSON Anda sebelum menerbitkan.
6. Pilih Exit Preview untuk kembali ke lensa kustom.

> **Note**
>
> Anda juga dapat melihat pratinjau lensa kustom dengan memilih Kirim & Pratinjau saat Membuat lensa khusus.

Menerbitkan lensa khusus untuk pertama kalinya

Untuk memublikasikan lensa kustom

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa kustom yang diinginkan dan pilih Terbitkan lensa.
4. Di kotak Nama versi, masukkan pengenal unik untuk perubahan versi. Nilai ini bisa sampai 32 karakter dan hanya boleh berisi karakter alfanumerik dan periode (“.”).
5. Pilih Publikasikan lensa kustom.

   Setelah lensa kustom diterbitkan, itu dalam status PUBLISH.

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

Menerbitkan pembaruan ke lensa kustom

Untuk mempublikasikan pembaruan ke lensa kustom yang ada

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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. Pilih Pilih file untuk memilih file JSON yang diperbarui dan pilih Kirim & Pratinjau untuk melihat pratinjau lensa kustom, atau Kirim untuk mengirimkan lensa khusus tanpa melihat pratinjau.

   Lensa khusus tidak boleh melebihi 500 KB.

   Setelah AWS WA Tool memvalidasi file JSON Anda, lensa kustom Anda ditampilkan di lensa Kustom dalam status DRAFT.
6. Pilih lensa kustom lagi dan pilih Terbitkan lensa.

7. Pilih Tinjau perubahan sebelum memublikasikan untuk memverifikasi bahwa perubahan yang dilakukan pada lensa kustom Anda sudah benar. Ini termasuk memvalidasi:

   - Nama lensa kustom
   - Nama-nama pilar
   - Pertanyaan baru, diperbarui, dan dihapus

   Pilih Berikutnya.

8. Tentukan jenis perubahan versi.

   Versi mayor

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

   Setiap beban kerja dengan lensa yang diterapkan akan diberi tahu bahwa versi baru dari lensa kustom tersedia.

   Perubahan versi utama tidak diterapkan secara otomatis ke beban kerja 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 pengenal unik untuk perubahan versi. Nilai ini bisa sampai 32 karakter dan hanya boleh berisi karakter alfanumerik dan periode (“.”).
10. Pilih Publikasikan lensa kustom.

    Setelah lensa kustom diterbitkan, itu dalam status PUBLISH.

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

Jika pembaruan adalah perubahan versi utama, beban kerja apa pun dengan versi lensa sebelumnya yang diterapkan akan diberi tahu bahwa versi baru tersedia dan diberi opsi untuk meningkatkan.

Pembaruan versi minor diterapkan secara otomatis tanpa pemberitahuan apa pun.

Anda dapat membuat hingga 100 versi lensa khusus.

Berbagi lensa kustom

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

Untuk berbagi lensa khusus dengan orang lain Akun AWS dan pengguna

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa khusus yang akan dibagikan dan pilih Lihat detail.
4. Pada Detail lensa halaman, pilih Berbagi. Kemudian pilih Buat dan Buat berbagi ke pengguna atau akun untuk membuat undangan berbagi lensa.
5. Masukkan Akun AWS ID 12 digit atau ARN pengguna yang ingin Anda bagikan lensa kustom.
6. Pilih Buat untuk mengirim undangan berbagi lensa ke yang ditentukan Akun AWS atau pengguna.

Anda dapat berbagi lensa khusus dengan hingga 300 Akun AWS atau pengguna.

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

> **Important**
>
> Sebelum berbagi lensa khusus dengan organisasi atau unit organisasi (OU), Anda harus mengaktifkan AWS Organizations akses.

Untuk berbagi lensa khusus dengan organisasi atau OU Anda

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.

2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa khusus yang akan dibagikan.
4. Pada Detail lensa halaman, pilih Berbagi. Kemudian pilih Create and Create shares to Organizations.
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 berbagi lensa khusus.

Untuk melihat siapa yang telah berbagi akses ke lensa kustom, pilih Berbagi dari Detail lensa halaman.

> **Sanggahan**
>
> Dengan berbagi lensa kustom Anda dengan yang lain Akun AWS, Anda mengakui bahwa AWS akan membuat lensa kustom Anda tersedia untuk akun lain tersebut. Akun-akun lain tersebut dapat terus mengakses dan menggunakan lensa kustom bersama Anda bahkan jika Anda menghapus lensa khusus dari lensa Anda sendiri Akun AWS atau menghentikan lensa Anda Akun AWS.

Menambahkan tag ke lensa khusus

Untuk menambahkan tag ke lensa kustom

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di panel navigasi kiri, pilih Lensa kustom.
3. Pilih lensa khusus yang ingin Anda perbarui.
4. Di bagian Tag, pilih Kelola Tag.
5. Pilih Tambahkan tag baru dan masukkan Kunci dan Nilai untuk setiap tag yang ingin Anda tambahkan.
6. Pilih Simpan.

Untuk menghapus tag, pilih Hapus di samping tag yang ingin Anda hapus.

Menghapus lensa khusus

Untuk menghapus lensa kustom

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

   Beban kerja yang ada dengan lensa yang diterapkan diberitahu bahwa lensa kustom telah dihapus, tetapi dapat terus menggunakannya. Lensa kustom tidak dapat lagi diterapkan pada beban kerja baru.

> **Sanggahan**
>
> Dengan berbagi lensa kustom Anda dengan yang lain Akun AWS, Anda mengakui bahwa AWS akan membuat lensa kustom Anda tersedia untuk akun lain tersebut. Akun-akun lain tersebut dapat terus mengakses dan menggunakan lensa kustom bersama Anda bahkan jika Anda menghapus lensa khusus dari lensa Anda sendiri Akun AWS atau menghentikan lensa Anda Akun AWS.

Spesifikasi format lensa

Lensa didefinisikan menggunakan format JSON tertentu. Saat Anda mulai membuat lensa khusus, Anda memiliki opsi untuk mengunduh file JSON template. 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 untuk digunakan. Ditetapkan oleh template, jangan berubah.
- `name`: Nama lensa. Namanya bisa sampai 128 karakter.

- `description`: Deskripsi teks lensa. Teks ini ditampilkan saat memilih lensa untuk ditambahkan selama pembuatan beban kerja, atau saat memilih lensa untuk diterapkan pada beban kerja yang ada nanti. Deskripsi dapat mencapai 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 AWS Well-Architected, menentukan pilar Anda sendiri, atau keduanya.

Anda dapat menentukan hingga 10 pilar dalam lensa khusus.

- `id`: ID untuk pilar. ID dapat 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 Framework, gunakan ID berikut:

  - `operationalExcellence`
  - `security`
  - `reliability`
  - `performance`
  - `costOptimization`
  - `sustainability`
- `name`: Nama pilar. Namanya bisa sampai 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 pilar di lensa khusus.

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

```
"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 khusus.

- `id`: ID untuk pilihan. ID dapat 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 bertindak sebagai `None of these` pilihan untuk pertanyaan.
- `title`: Judul pilihan. Judulnya bisa sampai 128 karakter.
- `helpfulResource displayText`: Opsional. Teks yang memberikan informasi bermanfaat tentang pilihan. Teks dapat mencapai 2048 karakter. Harus disertakan jika `helpfulResource url` ditentukan.
- `helpfulResource url`: Opsional. Sumber daya URL yang menjelaskan pilihan secara lebih rinci. URL harus dimulai dengan `http://` atau`https://`.
- `improvementPlan displayText`: Teks yang menjelaskan bagaimana pilihan dapat ditingkatkan. Teks dapat mencapai 2048 karakter. An `improvementPlan` diperlukan untuk setiap pilihan, kecuali untuk `None of these` pilihan.
- `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 `displayText` dan `url` nilai-nilai untuk sumber daya tambahan. Hingga lima sumber daya tambahan yang bermanfaat dan hingga lima item rencana peningkatan tambahan dapat ditentukan untuk suatu pilihan.
  - `displayText`: Opsional. Teks yang menjelaskan sumber daya yang bermanfaat atau rencana perbaikan. Teks dapat mencapai 2048 karakter. Harus disertakan jika `url` ditentukan.
  - `url`: Opsional. Sumber daya URL untuk sumber daya yang bermanfaat atau rencana peningkatan. URL harus dimulai dengan `http://` atau`https://`.

```
   "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_iplan_02.html"
                  },
                  {
                    "displayText": "This is the third piece of improvement plan
text.",
                    "url": "https://example.com/popt02_iplan_03.html"
                  }
                  {
                    "displayText": "This is the fourth piece of improvement plan
text.",
                    "url": "https://example.com/popt02_iplan_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_iplan_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 memetakan ke tingkat risiko untuk pertanyaan, atau`default`.

  Harus ada aturan `default` risiko untuk setiap pertanyaan.
- `risk`: Menunjukkan risiko yang terkait dengan kondisi tersebut. Nilai yang valid adalah `HIGH_RISK`, `MEDIUM_RISK`, dan `NO_RISK`.

Urutan aturan risiko Anda signifikan. `condition`Yang pertama mengevaluasi untuk `true` menetapkan risiko untuk pertanyaan. Pola umum untuk menerapkan aturan risiko adalah memulai dengan aturan Anda yang paling tidak berisiko (dan biasanya paling terperinci) dan lanjutkan ke aturan Anda yang paling berisiko (dan paling tidak spesifik).

Sebagai contoh:

```
"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 dipilih, tidak ada risiko.

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

Upgrade lensa

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

Upgrade lensa juga terjadi ketika lensa kustom yang telah Anda terapkan pada beban kerja atau template ulasan memiliki versi utama baru yang diterbitkan.

Upgrade lensa dapat terdiri dari kombinasi:

- Menambahkan pertanyaan baru atau praktik terbaik
- 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 dipertahankan.

> **Note**
>
> Anda tidak dapat membatalkan upgrade lensa. Setelah beban kerja ditingkatkan ke versi lensa terbaru, Anda tidak dapat kembali ke versi lensa sebelumnya.

Memilih upgrade lensa

Halaman Notifikasi menampilkan informasi untuk setiap beban kerja yang tidak menggunakan versi lensa terbaru.

Informasi berikut ditampilkan untuk setiap beban kerja:

Sumber daya

Nama beban kerja atau template ulasan.

Jenis sumber daya

Tipe sumber daya. Ini bisa berupa Workload atau template Review.

Sumber daya terkait

Nama lensa.

Jenis pemberitahuan

Jenis pemberitahuan pemutakhiran.

- 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 tersedia untuk upgrade, atau None jika lensa telah dihapus.

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

Memutakhirkan lensa

Lensa dapat ditingkatkan untuk beban kerja dan templat ulasan.

> **Note**
>
> Anda tidak dapat membatalkan upgrade lensa. Setelah template beban kerja atau ulasan ditingkatkan ke versi lensa terbaru, Anda tidak dapat kembali ke versi lensa sebelumnya.

Memutakhirkan lensa untuk beban kerja

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

   > **Note**
   >
   > Anda juga dapat memilih Lihat peningkatan yang tersedia dari tab Ikhtisar beban kerja.

2. Sebelum memutakhirkan lensa untuk beban kerja, tonggak sejarah dibuat untuk menyimpan status beban kerja Anda yang ada untuk referensi future. Masukkan nama unik untuk tonggak sejarah di bidang nama Milestone.
3. Pilih kotak Konfirmasi di sebelah Saya mengerti dan menerima perubahan ini dan pilih Simpan.

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

Memutakhirkan lensa untuk template ulasan

1. Untuk meng-upgrade lensa untuk template ulasan, pilih
2. Pada halaman Notifikasi, pilih templat ulasan untuk ditingkatkan, dan pilih Tingkatkan versi lensa. Informasi tentang apa yang berubah di setiap pilar ditampilkan.

   > **Note**
   >
   > Anda juga dapat memilih Lihat peningkatan yang tersedia dari tab Ikhtisar template ulasan.

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

Katalog Lensa

Katalog Lensa adalah kumpulan lensa resmi yang AWS dibuat yang menawarkan up-to-date teknologi dan praktik terbaik AWS WA Tool yang berfokus pada industri. Lensa ini tersedia untuk semua pengguna dan tidak memerlukan instalasi tambahan untuk digunakan.

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

Nama	Penjelasan
AWS Kerangka Well-Architected	Diterapkan secara default ke semua beban kerja. Kumpulan praktik terbaik arsitektur untuk merancang dan mengoperasikan sistem yang andal, aman, efisien, hemat biaya, dan berkelanjutan di cloud.
Mobilitas Terhubung	Praktik terbaik untuk mengintegrasikan teknologi ke dalam sistem transportasi dan meningkatkan pengalaman mobilitas secara keseluruhan.
Membangun Kontainer	Memberikan praktik terbaik pada desain kontainer dan proses pembuatan.
Analitik Data	Berisi wawasan yang AWS telah dikumpulkan dari studi kasus dunia nyata, dan 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 substansi f menggunakan teknologi modern dan praktik terbaik. DevOps
Pemerintah	Praktik terbaik untuk merancang dan memberikan layanan pemerintah di AWS.
Industri Kesehatan	Praktik dan panduan terbaik tentang cara merancang, menyebarkan, dan mengelola

Nama	Penjelasan
	beban kerja perawatan kesehatan Anda di. AWS Cloud
IoT	Praktik terbaik untuk mengelola beban kerja Internet of Things (IoT) Anda di. AWS
Penciptaan Nilai M&A	Menyediakan serangkaian pertanyaan tambahan untuk dipertimbangkan ketika mencari cara untuk mendorong pertumbuh an perusahaan seperti untuk merger ekuitas swasta dan aktivitas akuisisi.
Machine Learning	Praktik terbaik untuk mengelola sumber daya dan beban kerja Machine Learning Anda di AWS.
Migrasi:	Praktik terbaik untuk cara bermigrasi ke. AWS Cloud
SaaS	Berfokus pada merancang, menyebarkan, dan merancang perangkat lunak Anda sebagai beban kerja layanan (SaaS) di. AWS Cloud
GETAH	Prinsip-prinsip desain dan praktik terbaik untuk beban kerja SAP di. AWS Cloud
Aplikasi Tanpa Server	Praktik terbaik untuk membangun beban kerja tanpa server. AWS Meliputi skenario seperti layanan mikro RESTful, backend aplikasi seluler, pemrosesan aliran, dan aplikasi web.

Template ulasan

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 pengguna atau akun IAM lain, atau organisasi atau unit organisasi yang samaWilayah AWS. 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

Untuk membuat template ulasan

1. Pilih Tinjau template 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, lihatMenandai sumber daya AWS WA Tool Anda.
5. Pilih Selanjutnya.
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 template, di peringatan Mulai menjawab pertanyaan informasi, pilih lensa di dropdown 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

Untuk mengedit template ulasan

1. Pilih Tinjau template 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

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

Untuk berbagi template ulasan

1. Pilih Tinjau template 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 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 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

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, lihatthe section called "Memutakhirkan lensa".

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

Untuk menentukan beban kerja dari template ulasan

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

   > **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 lebih lanjut, lihatthe section called "Mendefinisikan 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 Selanjutnya.

Profil Well-Architected dan template ulasan dapat digunakan bersama-sama. 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

Untuk menghapus template ulasan

1. Pilih Tinjau template di panel navigasi kiri.
2. Di bagian Tinjau template, pilih template ulasan yang ingin Anda hapus dan di dropdown Tindakan, pilih Hapus.

> **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 pengguna, akun, atau organisasi IAM lainnya, mereka tidak akan dapat membuat beban kerja darinya.

Profil

Anda dapat membuat profil untuk menyediakan konteks bisnis Anda, dan mengidentifikasi tujuan yang ingin Anda capai saat melakukan tinjauan Well-Architected. AWS Well-Architected Toolmenggunakan informasi yang dikumpulkan dari profil Anda untuk membantu Anda fokus pada daftar pertanyaan prioritas yang relevan dengan bisnis Anda selama peninjauan beban kerja. Melampirkan profil ke beban kerja Anda juga membantu Anda melihat risiko mana yang diprioritaskan untuk Anda atasi dengan rencana peningkatan Anda.

Anda dapat membuat profil dari halaman Profil dan mengaitkannya dengan beban kerja baru, atau Anda dapat menambahkan profil ke beban kerja yang ada.

Membuat profil

Untuk membuat profil

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

   Untuk informasi selengkapnya tentang tag, lihatMenandai sumber daya AWS WA Tool Anda.
6. Pilih Save (Simpan). Pesan sukses muncul saat profil berhasil dibuat.

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

Mengedit profil

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 Ringkasan profil.
4. Buat pembaruan yang diperlukan untuk pertanyaan profil.
5. Pilih Save (Simpan).

Berbagi profil

Profil dapat dibagikan dengan pengguna atau akun, atau mereka 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 saham 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 saham 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, dan pilih Buat.

> **Important**
>
> Sebelum berbagi profil dengan organisasi atau unit organisasi (OU), Anda harus mengaktifkan AWS Organizations akses.

Menambahkan profil ke beban kerja

Anda dapat menambahkan profil ke beban kerja yang ada, atau saat menentukan beban kerja, untuk mempercepat proses peninjauan beban kerja. AWS WA Toolmenggunakan 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 “Mendefinisikan beban kerja”

Menambahkan profil ke beban kerja yang 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 lebih lanjut, lihat the section called “Membuat profil”.
4. Pilih Simpan.

Ringkasan Beban Kerja menampilkan sejumlah pertanyaan prioritas yang dijawab dan risiko prioritas berdasarkan informasi di profil terkait. Pilih Lanjutkan peninjauan 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

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

Menghapus profil dari beban kerja

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

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

Menghapus profil dari AWS WA Tool

Jika Anda membuat profil, Anda dapat menghapus profil dari daftar profil yang tersedia diAWS 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 dihapus, 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.

> **Sanggahan**
>
> Dengan membagikan profil Anda dengan orang lainAkun AWS, Anda mengakui bahwa profil Anda AWS akan tersedia untuk akun lain tersebut. Akun lain tersebut dapat terus mengakses dan menggunakan profil bersama Anda meskipun Anda menghapus profil dari profil Anda sendiri Akun AWS atau mengakhiri profil AndaAkun AWS.

Untuk menghapus profil dari daftar profil

1. Pilih Profil di panel navigasi kiri.
2. Pilih nama profil yang ingin Anda hapus.
3. Pilih Delete (Hapus).
4. Untuk mengkonfirmasi penghapusan, masukkan nama profil di bidang input teks.
5. Pilih Delete (Hapus).

Jika Anda ingin menyimpan profil di daftar Profil, tetapi menghapusnya dari beban kerja, lihatthe section called “Menghapus profil dari beban kerja”.

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, pilihSimpan tonggak.
2. DiNama tonggakkotak, 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. PilihSimpanuntuk 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, pilihTonggak sejarahdan 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 satuAkun 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 dibagikan dalam hal yang samaWilayah AWS.

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 “Memutakhirkan 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, lihatthe 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

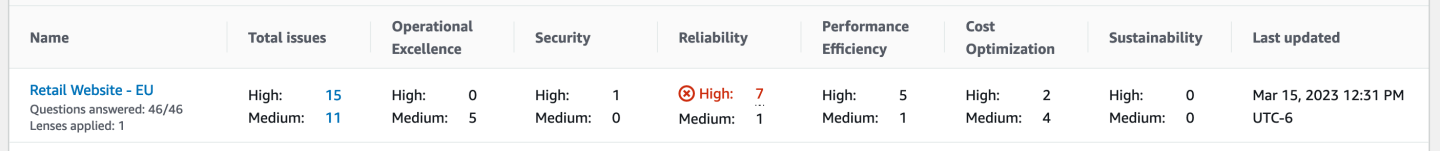
Masalah Kerangka Kerja Well-Architected per bagian pilar menunjukkan representasi grafis dari jumlah masalah risiko tinggi dan menengah berdasarkan pilar untuk semua beban kerja.

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

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

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

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

Topik

Perlindungan data di AWS Well-Architected Tool

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

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

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

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

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

Enkripsi diam

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

Enkripsi dalam bergerak

Semua data yang dikirim ke dan dari AWS WA Tool dienkripsi dalam perjalanan.

Cara AWS menggunakan data Anda

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

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

- Nama beban kerja
- Pemilik ulasan
- Environment
- Wilayah
- ID Akun
- Jenis industri

Tim AWS Well-Architected tidak memiliki akses ke:

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

Identitas dan manajemen akses untuk AWS Well-Architected Tool

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

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. AWS WA Tool

Pengguna layanan — Jika Anda menggunakan AWS WA Tool layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS WA Tool fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS WA Tool, lihat Memecahkan masalah AWS Well-Architected Tool identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas AWS WA Tool sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS WA Tool. Tugas Anda adalah menentukan AWS WA Tool fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM AWS WA Tool, lihatBagaimana AWS Well-Architected Tool bekerja dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke AWS WA Tool. Untuk melihat contoh kebijakan AWS WA Tool berbasis identitas yang dapat Anda gunakan di IAM, lihat. AWS Well-Architected Tool contoh kebijakan berbasis identitas

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas gabungan, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk

membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya andalkan kredensial sementara daripada membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami sarankan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Rotasikan kunci akses secara rutin untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

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

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Saat identitas terfederasi mengautentikasi, identitas tersebut akan dikaitkan dengan peran dan diberi izin yang ditentukan oleh peran tersebut. Untuk informasi tentang peran-peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda perlu mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengorelasikan izin yang diatur ke peran dalam IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut

menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.

- Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Saat Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat permintaan FAS, lihat Teruskan sesi akses.
- Peran layanan – Peran layanan adalah peran IAM yang diambil oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan dapat menggunakan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber

daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan dapat menentukan permintaan yang diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan konten dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat Memilih 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. 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 yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Daftar kontrol akses (ACL)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Developer Layanan Penyimpanan Ringkas Amazon.

Tipe kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di sebuah organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS

Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Beberapa jenis kebijakan

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

Bagaimana AWS Well-Architected Tool bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS WA Tool, pelajari fitur IAM yang tersedia untuk digunakan. AWS WA Tool

Fitur IAM yang dapat Anda gunakan AWS Well-Architected Tool

Fitur IAM	AWS WA Tool dukungan
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

Fitur IAM	AWS WA Tool dukungan
Izin pengguna utama	Ya
Peran layanan	Tidak
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS WA Tool dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas AWS WA Tool

Mendukung tindakan kebijakan	Ya

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

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

Menyertakan tindakan dalam suatu kebijakan untuk memberikan izin 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 yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama lintas akun ke kebijakan berbasis sumber daya bagian dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Izin diberikan dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, kebijakan berbasis identitas lainnya tidak diperlukan. Untuk informasi selengkapnya, lihat Perbedaan peran IAM dengan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Tindakan kebijakan untuk AWS WA Tool

Mendukung tindakan kebijakan	Ya

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

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

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

Tindakan kebijakan AWS WA Tool menggunakan awalan 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

`wellarchitected:DeleteWorkload` tindakan. 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 AWS WA Tool tindakan, 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 AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

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

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk mengindikasikan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis AWS WA Tool sumber daya dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS Well-Architected Tool dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan AWS Well-Architected Tool.

Sumber daya AWS WA Tool beban kerja memiliki ARN berikut:

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

Untuk informasi selengkapnya tentang format ARN, lihat Nama Sumber Daya Amazon (ARN) dan Ruang Nama AWS Layanan.

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

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

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

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

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

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

Untuk melihat daftar jenis AWS WA Tool sumber daya dan ARNnya, lihat Sumber Daya yang Ditentukan oleh AWS Well-Architected Tool dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang 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 spesifik layanan	Ya

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

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam satu pernyataan, atau beberapa kunci dalam satu elemen `Condition`, AWS akan mengevaluasinya dengan menggunakan operasi `AND`

logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag di Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

AWS WA Tool tidak menyediakan kunci kondisi khusus layanan apa pun, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Referensi Otorisasi Layanan.

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

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

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

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag di Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

ACL di AWS WA Tool

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengontrol pengguna utama (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun 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. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Pemberian tanda ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian, rancanglah kebijakan ABAC untuk mengizinkan operasi saat tag milik pengguna utama cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi di mana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan dengan 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 hanya untuk beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial terkait langkah-langkah penyiapan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan AWS WA Tool

Mendukung kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

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

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

Izin utama lintas layanan untuk AWS WA Tool

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Saat Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat permintaan FAS, lihat Teruskan sesi akses.

Peran layanan untuk AWS WA Tool

Mendukung peran layanan	Tidak

Peran layanan adalah sebuah 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 Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

Peran terkait layanan untuk AWS WA Tool

Mendukung peran terkait layanan	Tidak

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

Untuk detail tentang pembuatan atau pengelolaan peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Temukan sebuah layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

AWS Well-Architected Tool contoh kebijakan berbasis identitas

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi AWS WA Tool sumber daya. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. 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 read-only ke beban kerja
- Mengakses satu beban kerja

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di 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 melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – 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 Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda.

Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Menggunakan konsol AWS WA Tool

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

Untuk memastikan bahwa entitas tersebut masih dapat menggunakan AWS WA Tool konsol, lampirkan juga kebijakan AWS terkelola berikut ke entitas:

```
WellArchitectedConsoleReadOnlyAccess
```

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

```
WellArchitectedConsoleFullAccess
```

Untuk informasi selengkapnya, lihat Menambahkan Izin ke Pengguna dalam Panduan Pengguna IAM.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Memberikan akses penuh ke beban kerja

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

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

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

Memberikan akses read-only ke beban kerja

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

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

Mengakses satu beban kerja

Dalam contoh ini, Anda ingin memberi pengguna akses Akun AWS hanya-baca ke salah satu beban kerja Anda99999999999955555555555566666666, di Wilayah. `us-west-2` ID akun Anda adalah777788889999.

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

```
            "wellarchitected:List*"
        ],
        "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555666666666"
        }
    ]
}
```

AWS kebijakan terkelola untuk AWS Well-Architected Tool

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

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

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

Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: WellArchitectedConsoleFullAccess

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

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

Detail izin

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

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

AWS kebijakan terkelola: WellArchitectedConsoleReadOnlyAccess

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

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

Detail izin

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

AWS kebijakan terkelola: AWSWellArchitectedOrganizationsServiceRolePolicy

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

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

Detail izin

Kebijakan ini mencakup izin berikut.

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

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

```
    ]
}
```

AWS kebijakan terkelola: AWSWellArchitectedDiscoveryServiceRolePolicy

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

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

Detail izin

Kebijakan ini mencakup izin berikut.

- `trustedadvisor:DescribeChecks`— Daftar Trusted Advisor cek tersedia.
- `trustedadvisor:DescribeCheckItems`— Mengambil data Trusted Advisor pemeriksaan, termasuk status dan sumber daya yang ditandai oleh. Trusted Advisor
- `servicecatalog:GetApplication`— Mengambil detail AppRegistry aplikasi.
- `servicecatalog:ListAssociatedResources`—Daftar sumber daya yang terkait dengan AppRegistry aplikasi.
- `cloudformation:DescribeStacks`—Mendapat detail AWS CloudFormation tumpukan.
- `cloudformation:ListStackResources`—Daftar sumber daya yang terkait dengan AWS CloudFormation tumpukan.
- `resource-groups:ListGroupResources`—Daftar sumber daya dari a. ResourceGroup
- `tag:GetResources`— Diperlukan untuk ListGroupResources.
- `servicecatalog:CreateAttributeGroup`— Membuat grup atribut yang dikelola layanan bila 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 bila diperlukan.

```
{
 "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": [
    "servicecatalog:ListAssociatedResources",
    "servicecatalog:GetApplication",
    "servicecatalog:CreateAttributeGroup"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:AssociateAttributeGroup",
    "servicecatalog:DisassociateAttributeGroup"
   ],
   "Resource": [
```

```
    "arn:*:servicecatalog:*:*:/applications/*",
    "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:UpdateAttributeGroup",
    "servicecatalog:DeleteAttributeGroup"
   ],
   "Resource": [
    "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
   ]
  }
 ]
}
```

AWS WA Tool pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS WA Tool sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AWS WA Tool dokumen.

Perubahan	Deskripsi	Tanggal
AWS WA Tool mengubah kebijakan terkelola	Menambahkan `"wellarchitected:Export*"` ke `WellArchitectedConsoleReadOnlyAccess` .	22 Juni 2023
AWS WA Tool menambahkan kebijakan peran layanan	Ditambahkan `AWSWellArchitectedDiscoveryServiceRolePolicy` untuk memungkinkan AWS Well-Architected Tool untuk mengakses AWS layanan dan sumber daya yang berhubungan dengan AWS WA Tool sumber daya.	3 Mei 2023

Perubahan	Deskripsi	Tanggal
AWS WA Tool izin tambahan	Menambahkan tindakan baru `ListAWSServiceAccessForOrganization` untuk diberikan AWS WA Tool untuk memungkinkan untuk memeriksa apakah akses AWS layanan diaktifkan AWS WA Tool.	22 Juli 2022
AWS WA Tool mulai melacak perubahan	AWS WA Tool mulai melacak perubahan untuk kebijakan yang AWS dikelola.	22 Juli 2022

Memecahkan masalah AWS Well-Architected Tool identitas dan akses

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

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS WA Tool

Saya tidak berwenang untuk melakukan tindakan di AWS WA Tool

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

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

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

Untuk contoh ini, minta administrator memperbarui kebijakan agar Anda dapat mengakses `11112222333344445555666677778888` sumber daya menggunakan `wellarchitected:DeleteWorkload` tindakan tersebut.

Respon insiden di AWS Well-Architected Tool

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

AWS Masalah operasional dengan dampak luas diposting di AWS Service Health Dashboard.

Masalah operasional juga di-posting ke akun individu melalui AWS Health Dashboard. Untuk informasi tentang cara menggunakan AWS Health Dashboard, lihat Panduan AWS Health Pengguna.

Validasi kepatuhan untuk AWS Well-Architected Tool

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

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

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

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

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk mengevaluasi sumber daya AWS Anda dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Well-Architected Tool

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di AWS Well-Architected Tool

Sebagai layanan terkelola, AWS Well-Architected Tool dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur,

lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses 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.

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

Analisis konfigurasi dan kerentanan di AWS Well-Architected Tool

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Pencegahan confused deputy lintas layanan

Masalah deputi yang bingung adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan 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 pengguna utama layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan dalam kebijakan sumber daya untuk membatasi izin yang AWS Well-Architected Tool memberikan layanan lain ke sumber daya. Gunakan `aws:SourceArn` jika Anda hanya ingin satu sumber daya 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 kondisi konteks `aws:SourceArn` global dengan karakter wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:wellarchitected:*:123456789012:*`.

Jika `aws:SourceArn` nilainya tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global untuk membatasi izin.

Nilai `aws:SourceArn` harus berupa beban kerja atau lensa.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan AWS WA Tool untuk mencegah masalah wakil yang membingungkan.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "wellarchitected.amazonaws.com"
    },
    "Action": "wellarchitected:ActionName",
    "Resource": [
      "arn:aws:wellarchitected:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Berbagi AWS WA Tool sumber daya Anda

Untuk berbagi sumber daya yang Anda miliki, lakukan hal berikut:

- Aktifkan berbagi sumber daya dalam AWS Organizations (opsional)
- Bagikan beban kerja
- Bagikan lensa khusus
- Bagikan profil
- Bagikan templat ulasan

> **Catatan**
>
> - Berbagi sumber daya membuatnya tersedia untuk digunakan oleh kepala sekolah di luar Akun AWS yang menciptakan sumber daya. Berbagi tidak mengubah izin apa pun yang berlaku untuk sumber daya di akun yang membuatnya.
> - AWS WA Tooladalah layanan regional. Prinsipal yang Anda bagikan dapat mengakses pembagian sumber daya hanya Wilayah AWS di mana mereka dibuat.
> - Untuk berbagi sumber daya di Wilayah yang diperkenalkan setelah 20 Maret 2019, Anda dan yang dibagikan Akun AWS harus mengaktifkan Wilayah diAWS Management Console. Untuk informasi lebih lanjut, lihat Infrastruktur AWS Global.

Aktifkan berbagi sumber daya dalam AWS Organizations

Ketika akun Anda dikelola olehAWS Organizations, Anda dapat memanfaatkannya untuk berbagi sumber daya dengan lebih mudah. Dengan atau tanpa Organizations, pengguna dapat berbagi dengan akun individu. Namun, jika akun Anda berada dalam suatu organisasi, maka 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 organisasi, Anda harus terlebih dahulu menggunakan AWS WA Tool konsol atau AWS Command Line Interface (AWS CLI) untuk mengaktifkan berbagi denganAWS Organizations. Ketika Anda berbagi sumber daya di organisasi Anda, AWS WA Tool tidak mengirim undangan ke kepala sekolah. Prinsipal di organisasi Anda mendapatkan akses ke sumber daya bersama tanpa bertukar undangan.

Saat Anda mengaktifkan berbagi sumber daya dalam organisasi Anda, AWS WA Tool buat peran terkait layanan yang disebut. `AWSServiceRoleForWellArchitected` Peran ini hanya dapat diasumsikan oleh AWS WA Tool layanan, dan memberikan AWS WA Tool izin untuk mengambil informasi tentang organisasi yang menjadi anggotanya, dengan menggunakan kebijakan AWS terkelola. `AWSWellArchitectedOrganizationsServiceRolePolicy`

Jika Anda tidak perlu lagi berbagi sumber daya dengan seluruh organisasi atau OU, Anda dapat menonaktifkan berbagi sumber daya.

Persyaratan

- Anda dapat melakukan langkah-langkah ini hanya saat masuk sebagai prinsipal di akun manajemen organisasi.
- Organisasi harus mengaktifkan semua fitur. Untuk informasi selengkapnya, lihat Mengaktifkan semua fitur di organisasi Anda di Panduan AWS Organizations Pengguna.

> **Important**
>
> Anda harus mengaktifkan berbagi AWS Organizations dengan menggunakan AWS WA Tool konsol. Ini memastikan bahwa peran `AWSServiceRoleForWellArchitected` terkait layanan dibuat. Jika Anda mengaktifkan akses tepercaya AWS Organizations dengan menggunakan AWS Organizations konsol atau enable-aws-service-accessAWS CLIperintah, peran `AWSServiceRoleForWellArchitected` terkait layanan tidak dibuat, dan Anda tidak dapat berbagi sumber daya dalam organisasi Anda.

Untuk mengaktifkan berbagi sumber daya dalam organisasi Anda

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.

   Anda harus masuk sebagai kepala sekolah di akun manajemen organisasi.
2. Di panel navigasi kiri, pilih Pengaturan.
3. Pilih Aktifkan AWS Organizations dukungan.
4. Pilih Simpan pengaturan.

Untuk menonaktifkan berbagi sumber daya dalam organisasi Anda

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.

   Anda harus masuk sebagai kepala sekolah di akun manajemen organisasi.
2. Di panel navigasi kiri, pilih Pengaturan.
3. Batalkan pilihan Aktifkan AWS Organizations dukungan.
4. Pilih Simpan pengaturan.

Menandai 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 tanda. Topik ini menjelaskan tentang tanda dan menunjukkan kepada Anda cara membuatnya.

Daftar Isi

Dasar-dasar tanda

Tanda adalah sebuah label yang Anda tetapkan ke sebuah sumber daya AWS. Setiap tanda terdiri atas sebuah kunci dan sebuah nilai opsional, yang keduanya Anda tentukan.

Tanda 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 dengan segera mengidentifikasi sumber daya yang spesifik berdasarkan tanda yang telah Anda tetapkan pada sumber daya. Misalnya, Anda dapat menentukan satu set tanda untuk layanan AWS WA Tool untuk membantu Anda melacak setiap pemilik dan tingkat tumpukan layanan. Kami menyarankan agar Anda merancang serangkaian kunci tanda yang konsisten untuk setiap jenis sumber daya.

Selain itu, tanda tidak dapat menetapkan secara otomatis ke sumber daya Anda. Setelah Anda menambahkan sebuah tanda, Anda dapat mengedit kunci serta nilai tanda atau menghilangkan tanda dari sumber daya kapanpun yang Anda mau. Jika Anda menghapus sebuah sumber daya, tanda apapun untuk sumber daya tersebut juga dihapus.

Tanda tidak memiliki makna semantik pada AWS WA Tool dan diterjemahkan sebagai serangkaian karakter saja. Anda dapat mengatur nilai tanda menjadi sebuah string kosong, tetapi Anda tidak dapat mengatur nilai tanda menjadi nol. Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama.

Anda dapat bekerja dengan tanda menggunakan AWS Management Console, AWS CLI, dan API AWS WA Tool.

Jika Anda menggunakan AWS Identity and Access Management (IAM), Anda dapat mengontrol pengguna mana yang Akun AWS memiliki izin untuk membuat, mengedit, atau menghapus tag.

Menandai Sumber Daya Anda

Anda dapat menandai AWS WA Tool sumber daya baru atau yang sudah ada.

Jika menggunakan AWS WA Tool konsol, Anda dapat menerapkan tag ke sumber daya baru saat dibuat atau ke sumber daya yang ada kapan saja. Untuk beban kerja yang ada, Anda dapat menerapkan tag melalui tab Properties. Untuk lensa kustom, profil, dan templat ulasan yang ada, Anda dapat menerapkan tag melalui tab Ikhtisar.

Jika Anda menggunakan API AWS WA Tool, AWS CLI, atau AWS SDK, Anda dapat menerapkan tanda ke sumber daya baru dengan menggunakan parameter `tags` di pada tindakan API yang relevan atau ke sumber daya yang ada dengan menggunakan tindakan API `TagResource`. Untuk informasi lebih lanjut, lihat TagResource.

Selain itu, beberapa tindakan pembuatan sumber daya memungkinkan Anda menentukan tanda untuk sumber daya saat sumber daya diciptakan. Jika tanda tidak dapat diterapkan selama pembuatan sumber daya, proses pembuatan sumber daya akan gagal. Hal ini memastikan bahwa sumber daya yang ingin Anda tandai pada saat pembuatan dapat dibuat dengan tanda yang ditentukan atau justru tidak dibuat sama sekali. Jika Anda menandai sumber daya pada saat pembuatan, Anda tidak perlu menjalankan skrip penandaan khusus setelah pembuatan sumber daya.

Tabel berikut menjelaskan sumber daya AWS WA Tool yang dapat ditandai, dan sumber daya yang dapat ditandai saat dibuat.

Dukungan penandaan untuk sumber daya AWS WA Tool

Sumber daya	Mendukung tanda	Penyebaran tanda Support	Mendukung penandaan saat pembuatan (AWS WA Tool API, AWS CLI, AWS SDK)
AWS WA Toolbeban kerja	Ya	Tidak	Ya

Sumber daya	Mendukung tanda	Penyebaran tanda Support	Mendukung penandaan saat pembuatan (AWS WA Tool API, AWS CLI, AWS SDK)
AWS WA Toollensa kustom	Ya	Tidak	Ya
AWS WA Toolprofil	Ya	Tidak	Ya
AWS WA Tooltempl ate ulasan	Ya	Tidak	Ya

Batasan tanda

Batasan dasar berikut berlaku untuk tag:

- Jumlah maksimum tanda per sumber daya – 50
- Untuk setiap sumber daya, setiap kunci tag harus unik, dan setiap kunci tag hanya dapat memiliki satu nilai.
- Panjang kunci maksimum – 128 karakter Unicode dalam UTF-8
- Panjang nilai maksimum – 256 karakter Unicode dalam UTF-8
- Jika skema penandaan Anda digunakan di beberapa layanan dan sumber daya AWS, ingatlah bahwa layanan lain mungkin memiliki pembatasan pada karakter yang diizinkan. Karakter yang secara umum diperbolehkan adalah huruf, angka, spasi yang dapat diwakili dalam UTF-8, serta karakter berikut: + - = . _ : / @.
- Kunci dan nilai tanda sensitif huruf besar dan kecil.
- Jangan gunakan `aws:`, `AWS:`, atau kombinasi huruf besar atau huruf kecil dari itu semua sebagai prefiks untuk kunci atau nilai karena itu semua disimpan untuk penggunaan AWS. Anda tidak dapat menyunting atau menghapus kunci atau nilai tanda dengan prefiks ini. Tag dengan awalan ini tidak dihitung terhadap tags-per-resource batas Anda.

Bekerja dengan tanda menggunakan konsol

Menggunakan AWS WA Tool konsol, Anda dapat mengelola tag yang terkait dengan sumber daya baru atau yang sudah ada.

Menambahkan tanda pada pembuatan sumber daya individu

Anda dapat menambahkan tag ke AWS WA Tool sumber daya saat Anda membuatnya.

Penambahan dan penghapusan tanda pada sumber daya individu

AWS WA Toolmemungkinkan Anda untuk 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 ulasan.

Untuk menambah atau menghapus tag pada beban kerja

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di bilah navigasi, pilih Wilayah yang akan digunakan.
3. Di panel navigasi, pilih Beban kerja.
4. Pilih beban kerja yang akan dimodifikasi dan pilih Properties.
5. Di bagian Tag, pilih Kelola tag.
6. Tambah atau hapus tanda Anda sesuai kebutuhan.
   - Untuk menambahkan tag, pilih Tambahkan tag baru dan isi bidang Kunci dan Nilai.
   - Untuk menghapus sebuah tanda, pilih Hapus.
7. Ulangi proses ini untuk setiap tag yang ingin Anda tambahkan, ubah, atau hapus. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk menambah atau menghapus tag pada lensa kustom

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 khusus untuk dimodifikasi.
5. Di bagian Tag pada tab Ikhtisar, pilih Kelola tag.
6. Tambah atau hapus tanda Anda sesuai kebutuhan.
   - Untuk menambahkan tag, pilih Tambahkan tag baru dan isi bidang Kunci dan Nilai.
   - Untuk menghapus sebuah tanda, pilih Hapus.
7. Ulangi proses ini untuk setiap tag yang ingin Anda tambahkan, ubah, atau hapus. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk menambah atau menghapus tag pada profil

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol 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 dimodifikasi.
5. Di bagian Tag pada tab Ikhtisar, pilih Kelola tag.
6. Tambah atau hapus tanda Anda sesuai kebutuhan.
   - Untuk menambahkan tag, pilih Tambahkan tag baru dan isi bidang Kunci dan Nilai.
   - Untuk menghapus sebuah tanda, pilih Hapus.
7. Ulangi proses ini untuk setiap tag yang ingin Anda tambahkan, ubah, atau hapus. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk menambah atau menghapus tag pada template ulasan

1. Masuk ke AWS Management Console dan buka AWS Well-Architected Tool konsol di https://console.aws.amazon.com/wellarchitected/.
2. Di bilah navigasi, pilih Wilayah yang akan digunakan.
3. Di panel navigasi, pilih Tinjau templat.
4. Pilih nama template ulasan yang akan dimodifikasi.
5. Di bagian Tag pada tab Ikhtisar, pilih Kelola tag.
6. Tambah atau hapus tanda Anda sesuai kebutuhan.

- Untuk menambahkan tag, pilih Tambahkan tag baru dan isi bidang Kunci dan Nilai.
- Untuk menghapus sebuah tanda, pilih Hapus.

7. Ulangi proses ini untuk setiap tag yang ingin Anda tambahkan, ubah, atau hapus. Pilih Simpan untuk menyimpan perubahan Anda.

Bekerja dengan tag menggunakan API

Gunakan operasi AWS WA Tool API berikut untuk menambahkan, memperbarui, membuat daftar, dan menghapus tag untuk sumber daya Anda.

Dukungan penandaan untuk sumber daya AWS WA Tool

Tugas	Tindakan API
Penambahan atau penimpaan satu tanda atau lebih.	TagResource
Hapus satu atau beberapa tanda.	UntagResource
Daftar tag untuk sumber daya.	ListTagsForResource

Beberapa tindakan pembuatan sumber daya memungkinkan Anda untuk menentukan tanda saat membuat sumber daya. Tindakan berikut mendukung penandaan saat pembuatan.

Tugas	Tindakan API
Buat beban kerja	CreateWorkload
Impor lensa baru	ImportLens
Membuat profil	CreateProfile
Buat template ulasan	CreateReviewTemplate

Mencatat panggilan API AWS WA Tool dengan AWS CloudTrail

AWS Well-Architected Toolterintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, atauAWS layanan diAWS WA Tool. CloudTrail menangkap semua panggilan untukAWS WA Tool sebagai kejadian. Panggilan yang direkam mencakup panggilan dari AWS WA Tool konsol dan panggilan kode ke operasi API AWS WA Tool ini. Jika membuat jejak, Anda dapat mengaktifkan pengiriman tindakan berkelanjutan CloudTrail ke bucket Amazon S3, termasuk tindakan untukAWS WA Tool. Jika Anda tidak dapat mengonfigurasi jejak, Anda masih dapat melihat tindakan terbaru dalam CloudTrail konsol di Riwayat peristiwa. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuatAWS WA Tool, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail lainnya.

Untuk mempelajari lebih lanjut CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

AWS WA Toolinformasi dalam CloudTrail

CloudTrail diaktifkan pada AndaAkun AWS saat Anda membuat akun. Ketika aktivitas terjadi diAWS WA Tool,, aktivitas tersebut dicatat dalam CloudTrail peristiwa bersama peristiwaAWS layanan lainnya di Riwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat Kejadian dengan Riwayat CloudTrail Kejadian.

Untuk catatan berkelanjutan tentang peristiwa di Akun AWS, termasuk peristiwa untuk AWS WA Tool, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim berkas ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasiAWS layanan lainnya untuk menganalisis lebih lanjut dan bertindak berdasarkan data kejadian yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Ikhtisar untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail

- Menerima Berkas CloudTrail Log dari Beberapa Wilayah dan Menerima Berkas CloudTrail Log dari Beberapa Akun

SemuaAWS WA Tool tindakan dicatat oleh CloudTrail dan didokumentasikan dalam Tindakan Ditetapkan olehAWS Well-Architected Tool. Misalnya, panggilan ke`CreateWorkload`,`DeleteWorkload`, dan`CreateWorkloadShare` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Jika permintaan tersebut dibuat dengan kredensial pengguna atau.
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.
- Bahwa permintaan dibuat oleh layanan AWS lain.

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Memahami entri file log AWS WA Tool

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail berkas log berisi satu atau beberapa entri. Sebuah peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail Berkas log bukan merupakan jejak terurut dari panggilan publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan`CreateWorkload` tindakan.

```
   {
    "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 Toolmengirimkan acara ke Amazon EventBridge ketika tindakan diambil pada sumber Well-Architected. Anda dapat menggunakan EventBridge dan peristiwa ini untuk menulis aturan yang mengambil tindakan, seperti memberi tahu Anda, ketika terjadi perubahan sumber daya. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan Amazon EventBridge?

> **Note**
>
> Peristiwa disampaikan dengan dasar upaya-terbaik.

Tindakan berikut menghasilkan EventBridge peristiwa:

- terkait beban kerja
  - Membuat atau menghapus beban kerja
  - Membuat tonggak
  - Memperbarui properti beban kerja
  - Berbagi atau membatalkan berbagi beban kerja
  - Memperbarui status undangan berbagi
  - Menambahkan atau menghapus tag
  - Memperbarui jawaban
  - Memperbarui catatan tinjauan
  - Menambahkan atau melepas lensa dari beban kerja
- Lensa terkait
  - Mengimpor atau mengekspor lensa khusus
  - Menerbitkan lensa kustom
  - Menghapus lensa kustom
  - Berbagi atau membatalkan berbagi lensa kustom
  - Memperbarui status undangan berbagi
  - Menambahkan atau melepas lensa dari beban kerja

Contoh peristiwa dariAWS 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":"AROA4JUSXMN5ZR6S7LZNP:sample-user",
        "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "sessionContext":{
           "sessionIssuer":{
              "type":"Role",
              "principalId":"AROA4JUSXMN5ZR6S7LZNP",
              "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":"AROA4JUSXMN5ZR6S7LZNP:example-user",
         "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
         "accountId":"123456789012",
         "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
         "sessionContext":{
            "sessionIssuer":{
               "type":"Role",
               "principalId":"AROA4JUSXMN5ZR6S7LZNP",
               "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"
   }
}
```

Riwayat dokumen

Tabel berikut menjelaskan dokumentasi untuk rilis iniAWS Well-Architected Tool.

- Versi API: terbaru
- Pembaruan dokumentasi terbaru: 26 November 2023

Perubahan	Deskripsi	Tanggal
Fungsionalitas yang diperbarui	Rilis ini menambahkan fitur Katalog Lensa keAWS WA Tool.	26 November 2023
Fungsionalitas yang diperbarui	Rilis ini menambahkan fitur Template Ulasan keAWS WA Tool.	Oktober 3, 2023
WellArchitectedConsoleReadOnlyAccess kebijakan terkelola diperbarui	Menambahkan `"wellarchitected:ExportLens"` ke `WellArchitectedConsoleReadOnlyAccess` .	Juni 22, 2023
Fungsionalitas yang diperbarui	Rilis ini menambahkan fitur Profil keAWS WA Tool.	13 Juni 2023
Fungsionalitas yang diperbarui	Rilis ini meningkatkan AWS Trusted Advisor dan AWS Service Catalog AppRegistry integrasi, dan menambahkan `AWSWellArchitectedDiscoveryServiceRolePolicy` ke kebijakan AWS terkelola.	3 Mei 2023
Pembaruan konten	Halaman dasbor diperbarui untuk menyertakan rincian risiko dan informasi rencana	30 Maret 2023

	perbaikan. Kemampuan untuk membuat laporan beban kerja terkonsolidasi juga ditambahkan.	
Pembaruan konten	Nama WellArchitectedConsoleReadOnlyAccess kebijakan yang dikoreksi.	19 Januari 2023
Memperbarui panduan IAM untuk AWS WA Tool	Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM.	4 Januari 2023
Fungsionalitas yang diperbarui	Rilis ini menghapus lensa FTR dari alat.	14 Desember 2022
Fungsionalitas yang diperbarui	Rilis ini menambahkan AWS Trusted Advisor dan AWS Service Catalog AppRegistry integrasi.	November 7, 2022
Pembaruan konten	Memperbaiki masalah dalam contoh JSON lensa khusus untuk. `choices`	September 29, 2022
Pembaruan konten	`choices`Bagian spesifikasi JSON lensa kustom telah diperbarui.	Agustus 2, 2022

Fungsionalitas yang diperbarui	Rilis ini menambahkan perubahan pelacakan untuk kebijakan yang AWS dikelola dan menambahkan tindakan baru untuk memberikan `ListAWSServiceAccessForOrganization` izin kepada`AWSWellArchitectedOrganizationsServiceRolePolicy` .	22 Juli 2022
Berbagi organisasi ditambahkan	Rilis ini menambahkan kemampuan untuk berbagi beban kerja dan lensa khusus dengan unit organisasi dan organisasi (OU).	30 Juni 2022
Fungsionalitas yang diperbarui	Rilis ini menambahkan kemampuan untuk menentukan sumber daya tambahan untuk pilihan dalam lensa kustom, untuk melihat pratinjau lensa kustom sebelum menerbitkannya, dan menambahkan tag ke lensa kustom.	21 Juni 2022
Fungsionalitas yang diperbarui	Rilis ini menambahkan kemampuan untuk mengakses komunitas AWS Well-Architected di Re:post. AWS	31 Mei 2022
Fungsionalitas yang diperbarui	Rilis ini menambahkan pilar keberlanjutan dan pembaruan kecil untuk Tutorial.	31 Maret 2022

EventBridge dukungan ditambahkan	AWS WA Toolsekarang mengirimkan acara ke Amazon EventBridge ketika perubahan dilakukan ke sumber daya Well-Architected.	Maret 3, 2022
Lensa khusus ditambahkan	Kemampuan untuk menambahkan lensa khusus telah ditambahkan.	29 November 2021
Fungsionalitas yang diperbarui	Praktik terbaik individu sekarang dapat ditandai sebagai tidak berlaku.	14 Juli 2021
Penandaan sumber daya tersedia	Rilis ini menambahk an kemampuan untuk menambahkan tag ke beban kerja.	3 Maret 2021
API sekarang tersedia	Rilis ini menambahkan AWS WA Tool API. AWS CloudTrai linformasi logging ditambahk an.	16 Desember 2020
Fungsionalitas yang 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 meng-upgrade beban kerja untuk menggunak an lensa baru yang Anda tidak dapat kembali ke versi sebelumnya.	8 Juli 2020

Pembaruan konten	Berbagi yang diklarifikasi Wilayah AWS diperkenalkan setelah 20 Maret 2019.	24 Juni 2020
Fungsionalitas yang 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) ditambahk an.	12 Juni 2020
Pembaruan konten	Bagian tentang cara AWS menggunakan data Anda ditambahkan.	21 Mei 2020
Fungsionalitas yang diperbarui	Rilis ini menambahkan pemilik ulasan ke beban kerja.	1 April 2020
Fungsionalitas yang diperbarui	Rilis ini menambahkan link diagram arsitektur ke beban kerja.	10 Maret 2020
Pembaruan konten	Mengklarifikasi bahwa pembagian beban kerja bersifat Wilayah AWS -spesifik .	10 Januari 2020
Fungsionalitas yang diperbarui	Rilis ini menambahkan berbagi beban kerja.	9 Januari 2020
Pembaruan konten	Bagian keamanan diperbarui dengan panduan terbaru.	Desember 6, 2019

Fungsionalitas yang diperbarui	Rilis ini membuat bidang industri opsional saat menentukan beban kerja.	19 Agustus 2019
Fungsionalitas yang diperbarui	Rilis ini menambahkan item rencana perbaikan ke laporan beban kerja.	29 Juli 2019
Fungsionalitas yang diperbarui	Rilis menambahkan DeleteWorkload tindakan ke kebijakan.	18 Juli 2019
Pembaruan konten	Konten dalam panduan ini telah diperbarui dengan perbaikan kecil.	19 Juni 2019
Pembaruan konten	Konten dalam panduan ini telah diperbarui dengan perbaikan kecil.	30 Mei 2019
Fungsionalitas yang diperbarui	Rilis ini mendukung peningkatan versi kerangka kerja yang digunakan untuk tinjauan beban kerja.	1 Mei 2019
Fungsionalitas yang diperbarui	Rilis ini menambahkan kemampuan untuk menentukan non- Wilayah AWS saat mendefinisikan beban kerja.	14 Februari 2019
AWS Well-Architected Toolketersediaan umum	Rilis ini memperkenalkan. AWS Well-Architected Tool	29 November 2018

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS