Guia do usuário

AWS Well-Architected Tool

AWS Well-Architected Tool: Guia do usuário

Table of Contents

..... vii
O que é o AWS Well-Architected Tool? 1
O que é o AWS Well-Architected Framework? 2
Glossário da AWS Well-Architected Tool 2
Conceitos básicos 4
Conceder acesso ao AWS WA Tool 4
Ativando integrações 5
Ativar o AppRegistry 6
Ativação do Trusted Advisor 6
Definir uma workload 14
Documentar uma workload 17
Analisar uma workload 18
Visualizar verificações do Trusted Advisor 20
Salvar um marco 22
Tutorial: documentar uma workload 23
Etapa 1: definir uma workload 23
Etapa 2: documentar o estado da workload 24
Etapa 3: Revisar o plano de aprimoramento 28
Etapa 4: Faça melhorias e avalie o progresso 30
Workloads no AWS Well-Architected Tool 32
Problemas de alto risco (HRI) e problemas de risco médio (MRI) 33
Definir uma workload 34
Visualizar uma workload 35
Editar uma workload 35
Compartilhar uma workload 36
Considerações sobre compartilhamento 39
Excluir acesso compartilhado 40
Modificar o acesso compartilhado 40
Aceitar e rejeitar convites 41
Excluir uma workload 42
Gerar um relatório de workload 43
Visualizar detalhes da workload 43
Guia Visão geral 44
Guia Etapas 44

Guia Propriedades ... 45
Guia Compartilhamentos ... 45
Lentes ... 47
Adicionar uma lente ... 47
Remover uma lente ... 48
Visualizar detalhes da lente ... 48
Guia Visão geral ... 49
Guia Plano de melhoria ... 49
Guia Compartilhamentos ... 49
Lentes personalizadas ... 49
Visualizar lentes personalizadas ... 50
Criar uma lente personalizada ... 51
Prévia de uma lente personalizada ... 52
Publicar uma lente personalizada ... 53
Publicar uma atualização de lente ... 53
Compartilhar uma lente ... 55
Adicionar tags a uma lente ... 57
Excluir uma lente ... 57
Especificação do formato da lente ... 58
Atualizações de lente ... 65
Determinar as lentes para atualizar ... 65
Fazer upgrade de uma lente ... 66
Catálogo de lentes ... 67
Modelos de avaliação ... 70
Criar um modelo de avaliação ... 70
Editar um modelo de avaliação ... 71
Compartilhar um modelo de avaliação ... 72
Definir uma workload com base em um modelo ... 73
Excluir um modelo de avaliação ... 74
Perfis ... 76
Criar um perfil ... 76
Edição de um perfil ... 77
Edição de um perfil ... 77
Adicionar um perfil a uma workload ... 78
Remover um perfil de uma workload ... 78
Excluir um perfil ... 79

Jira ... 80
Configurar o conector ... 81
Configurar o conector do ... 82
Sincronizar uma workload ... 84
Desinstalar o conector ... 85
Marcos ... 87
Salvar um marco ... 87
Visualizar marcos ... 87
Gerar um relatório de marcos ... 88
Compartilhar convites ... 89
Aceitando um convite de compartilhamento ... 90
Rejeitar um convite de compartilhamento ... 91
Notificações ... 92
Notificações de lentes ... 92
Notificações de perfil ... 92
Painel ... 94
Resumo ... 94
Problemas do Well-Architected Framework por pilar ... 94
Problemas do Well-Architected Framework por workload ... 95
Problemas do Well-Architected Framework por item do plano de melhoria ... 96
Segurança ... 98
Proteção de dados ... 99
Criptografia em repouso ... 100
Criptografia em trânsito ... 100
Como a AWS usa seus dados ... 100
Gerenciamento de Identidade e Acesso ... 101
Público ... 101
Como autenticar com identidades ... 102
Gerenciar o acesso usando políticas ... 106
Como o AWS Well-Architected Tool funciona com o IAM ... 108
Exemplos de políticas baseadas em identidade ... 116
Políticas gerenciadas pela AWS ... 122
Solução de problemas ... 128
Resposta a incidentes ... 129
Validação de conformidade ... 129
Resiliência ... 131

Segurança da infraestrutura 131
Análise de configuração e vulnerabilidade 132
Prevenção contra o ataque do “substituto confuso” em todos os serviços 132
Compartilhar seus recursos 134
Ativar o compartilhamento de recursos dentro da AWS Organizations 134
Marcando seus Recursos 137
Conceitos Básicos de Tags 137
Marcando seus Recursos 138
Restrições de tag 139
Trabalhando com tags usando o console 139
Adicionar tags a um recurso individual na criação 140
Adicionando e excluindo tags em um recurso individual 140
Trabalhar com tags usando a API 142
Registro em log 143
Informações do AWS WA Tool no CloudTrail 143
Noções básicas sobre entradas de arquivos de log do AWS WA Tool 144
EventBridge 147
Exemplo de eventos do AWS WA Tool 148
Histórico do documentos 152
Glossário da AWS 159

Lançamos uma nova versão do Well-Architected Framework. Também adicionamos lentes novas e atualizadas ao Catálogo de Lentes. Saiba mais sobre as mudanças.

O que é o AWS Well-Architected Tool?

O AWS Well-Architected Tool (AWS WA Tool) é um serviço na nuvem que oferece um processo consistente para avaliar sua arquitetura usando as práticas recomendadas da AWS. O AWS WA Tool ajuda você em todo o ciclo de vida do produto fazendo o seguinte:

- Auxiliando na documentação das decisões tomadas
- Fornecendo recomendações para melhorar sua carga de trabalho com base nas melhores práticas
- Orientando você para tornar suas cargas de trabalho mais confiáveis, seguras, eficientes e econômicas

Você pode usar o AWS WA Tool para documentar e medir a workload usando as práticas recomendadas do AWS Well-Architected Framework. Essas práticas recomendadas foram desenvolvidas pelos arquitetos de soluções da AWS com base em seus anos de experiência na criação de soluções em uma ampla variedade de empresas. A estrutura fornece uma abordagem consistente para medir arquiteturas e oferece orientação para implementar projetos que são dimensionados conforme suas necessidades ao longo do tempo.

Além das práticas recomendadas da AWS, você pode usar lentes personalizadas para medir a workload usando suas próprias práticas recomendadas. Você pode adaptar as perguntas em uma lente personalizada para que sejam específicas de uma determinada tecnologia ou para ajudá-lo a atender às necessidades de governança da sua organização. As lentes personalizadas ampliam a orientação fornecida pelas lentes da AWS.

As integrações com o AWS Trusted Advisor e o AWS Service Catalog AppRegistry ajudam você a descobrir mais facilmente as informações necessárias para responder às perguntas de avaliação do AWS Well-Architected Tool.

Esse serviço é destinado aos envolvidos no desenvolvimento de produtos técnicos, como diretores de tecnologia (CTOs), arquitetos, desenvolvedores e membros da equipe de operações. Os clientes da AWS usam o AWS WA Tool para documentar suas arquiteturas, fornecer governança de lançamento de produtos e entender e gerenciar os riscos em seu portfólio de tecnologia.

Tópicos

- O que é o AWS Well-Architected Framework?
- Glossário da AWS Well-Architected Tool

O que é o AWS Well-Architected Framework?

O AWS Well-Architected Framework documenta um conjunto de perguntas fundamentais que permitem que você entenda como uma arquitetura específica se alinha às práticas recomendadas de nuvem. O framework fornece uma abordagem consistente para avaliar sistemas com base nas qualidades esperadas dos sistemas modernos baseados em nuvem. De acordo com o estado de sua arquitetura, a estrutura sugere melhorias que você pode fazer para alcançar melhor essas qualidades.

Ao usar o Framework, você conhecerá as melhores práticas de arquitetura para criar e operar sistemas confiáveis, seguros e econômicos na nuvem. Ele fornece uma maneira de avaliar de forma consistente suas arquiteturas em relação às práticas recomendadas e identificar áreas para melhorias. A estrutura é baseada em seis pilares: excelência operacional, segurança, confiabilidade, eficiência de desempenho, otimização de custos e sustentabilidade.

Ao projetar cargas de trabalho, você faz trocas entre esses pilares de acordo com suas necessidades comerciais. Essas decisões comerciais ajudam a determinar suas prioridades de engenharia. Em ambientes de desenvolvimento, é possível otimizar para reduzir custos em detrimento da confiabilidade. Em soluções de missão crítica, você pode otimizar a confiabilidade e estar disposto a aceitar um aumento dos custos. Em soluções de comércio eletrônico, você pode priorizar o desempenho, já que a satisfação do cliente pode impulsionar o aumento da receita. Segurança e excelência operacional geralmente não se envolvem em trocas com os outros pilares.

Para obter mais informações sobre o framework, acesse o site do AWS Well-Architected.

Glossário da AWS Well-Architected Tool

A seguir é apresentada a definição de termos comuns usados no AWS WA Tool e no AWS Well-Architected Framework.

- Uma carga de trabalho identifica um conjunto de componentes que fornecem valor comercial. A carga de trabalho geralmente é o nível de detalhes sobre o qual os líderes comerciais e tecnológicos se comunicam. Exemplos de cargas de trabalho incluem sites de marketing, sites de comércio eletrônico, o back-end de um aplicativo móvel e plataformas de análises. As cargas de trabalho variam no nível de complexidade da arquitetura. Elas podem ser simples, como um site estático, ou complexas, como arquiteturas de microsserviços com vários datastores e muitos componentes.

- Os marcos marcam as principais alterações em sua arquitetura à medida que ela evolui ao longo do ciclo de vida do produto: design, testes, entrada em operação e produção.
- As perspectivas oferecem uma maneira de você medir de forma consistente suas arquiteturas em relação às melhores práticas e identificar áreas para melhoria.

  Além das lentes fornecidas pela AWS, você também pode criar e usar suas próprias lentes ou usar as que foram compartilhadas com você.
- Os problemas de alto risco (HRIs) são escolhas arquitetônicas e operacionais que a AWS descobriu que podem resultar em um impacto negativo significativo para uma empresa. Esses HRI podem afetar ativos, indivíduos e operações organizacionais.
- Os problemas de risco médio (MRIs) são escolhas arquitetônicas e operacionais que a AWS descobriu que podem afetar negativamente os negócios, mas em menor grau do que os HRIs.

  Para obter informações adicionais, consulte Problemas de alto risco (HRI) e problemas de risco médio (MRI).

Conceitos básicos do AWS Well-Architected Tool

Para começar a usar o AWS Well-Architected Tool, primeiro forneça as permissões apropriadas a usuários, grupos e funções e ative o suporte para os Serviços da AWS que você deseja usar com o AWS WA Tool. Em seguida, defina e documente uma workload. Também é possível salvar um marco do estado atual de uma workload.

Os seguintes tópicos explicam como começar a usar o AWS WA Tool. Para ver um tutorial passo a passo mostrando como usar o AWS Well-Architected Tool, consulte o Tutorial: Documentar uma workload do AWS Well-Architected Tool.

Tópicos

- Fornecer aos usuários, grupos ou perfis o AWS WA Tool
- Ativar o suporte no AWS WA Tool para outros serviços da AWS
- Definir uma workload no AWS WA Tool
- Documentar uma workload no AWS WA Tool
- Analisar uma workload com o AWS Well-Architected Framework
- Visualizar verificações do Trusted Advisor de sua workload
- Salvar um marco referente a uma workload no AWS WA Tool

Fornecer aos usuários, grupos ou perfis o AWS WA Tool

Você pode conceder a usuários, grupos ou funções controle total ou acesso somente leitura ao AWS Well-Architected Tool.

Fornece acesso total ao AWS WA Tool

1. Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

   - Usuários e grupos no AWS IAM Identity Center:

     Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.

   - Usuários gerenciados no IAM com provedor de identidades:

Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

2. Para conceder controle total, aplique a política WellArchitectedConsoleFullAccess gerenciada ao conjunto de permissões ou à função.

   O acesso total permite que a entidade principal execute todas as ações no AWS WA Tool. Esse acesso é necessário para definir workloads, excluir workloads, visualizar workloads, atualizar workloads, compartilhar workloads, criar lentes personalizadas e compartilhar lentes personalizadas.

3. Para conceder acesso somente leitura, aplique a política gerenciada WellArchitectedConsoleReadOnlyAccess ao conjunto de permissões ou ao perfil. As entidades principais com esse perfil só podem visualizar os recursos.

Para obter mais informações sobre essas políticas, consulte Políticas gerenciadas pela AWS para o AWS Well-Architected Tool.

Ativar o suporte no AWS WA Tool para outros serviços da AWS

A ativação do acesso à organização permite que o AWS Well-Architected Tool reúna informações sobre a estrutura da sua organização para compartilhar recursos com mais facilidade (consulte the section called “Ativar o compartilhamento de recursos dentro da AWS Organizations” para obter mais informações). A ativação do suporte do Discovery reúne informações do AWS Trusted Advisor, do AWS Service Catalog AppRegistry e de recursos relacionados (como pilhas do AWS CloudFormation em coleções de recursos do AppRegistry) para ajudar a descobrir mais facilmente as informações necessárias para responder às perguntas de avaliação do Well-Architected e personalizar as verificações do Trusted Advisor para uma workload.

A ativação do suporte ao AWS Organizations ou a ativação do suporte ao Discovery cria automaticamente uma função vinculada ao serviço em sua conta.

Para ativar o suporte a outros serviços com os quais o AWS WA Tool pode interagir, navegue até Configurações.

1. Para coletar informações do AWS Organizations, ative Ativar suporte do AWS Organizations.
2. Ative o suporte do Activate Discovery para coletar informações de outros serviços e recursos da AWS.
3. Selecione Exibir permissões de função para visualizar as permissões de função vinculadas ao serviço ou as políticas de relacionamento de confiança.
4. Selecione Salvar configurações.

Ativar o AppRegistry para uma workload

Usar o AppRegistry é opcional, e os clientes do AWS Business and Enterprise Support podem ativá-lo por workload.

Sempre que o suporte ao Discovery é ativado e o AppRegistry é associado a uma workload nova ou existente, o AWS Well-Architected Tool cria um grupo de atributos gerenciado pelo serviço. O grupo de atributos Metadados no AppRegistry contém o ARN da workload, o nome da workload e os riscos associados à workload.

- Quando o suporte ao Discovery é ativado, sempre que há uma alteração na workload, o grupo de atributos é atualizado.
- Quando o suporte ao Discovery é desativado ou a aplicação é removida da workload, as informações da workload são removidas do AWS Service Catalog.

Se quiser que uma aplicação do AppRegistry conduza os dados obtidos do Trusted Advisor, defina a Definição do recurso da workload como AppRegistry ou Tudo. Crie funções para todas as contas que possuem recursos em seu aplicativo seguindo as diretrizes em the section called “Ativando Trusted Advisor no IAM”.

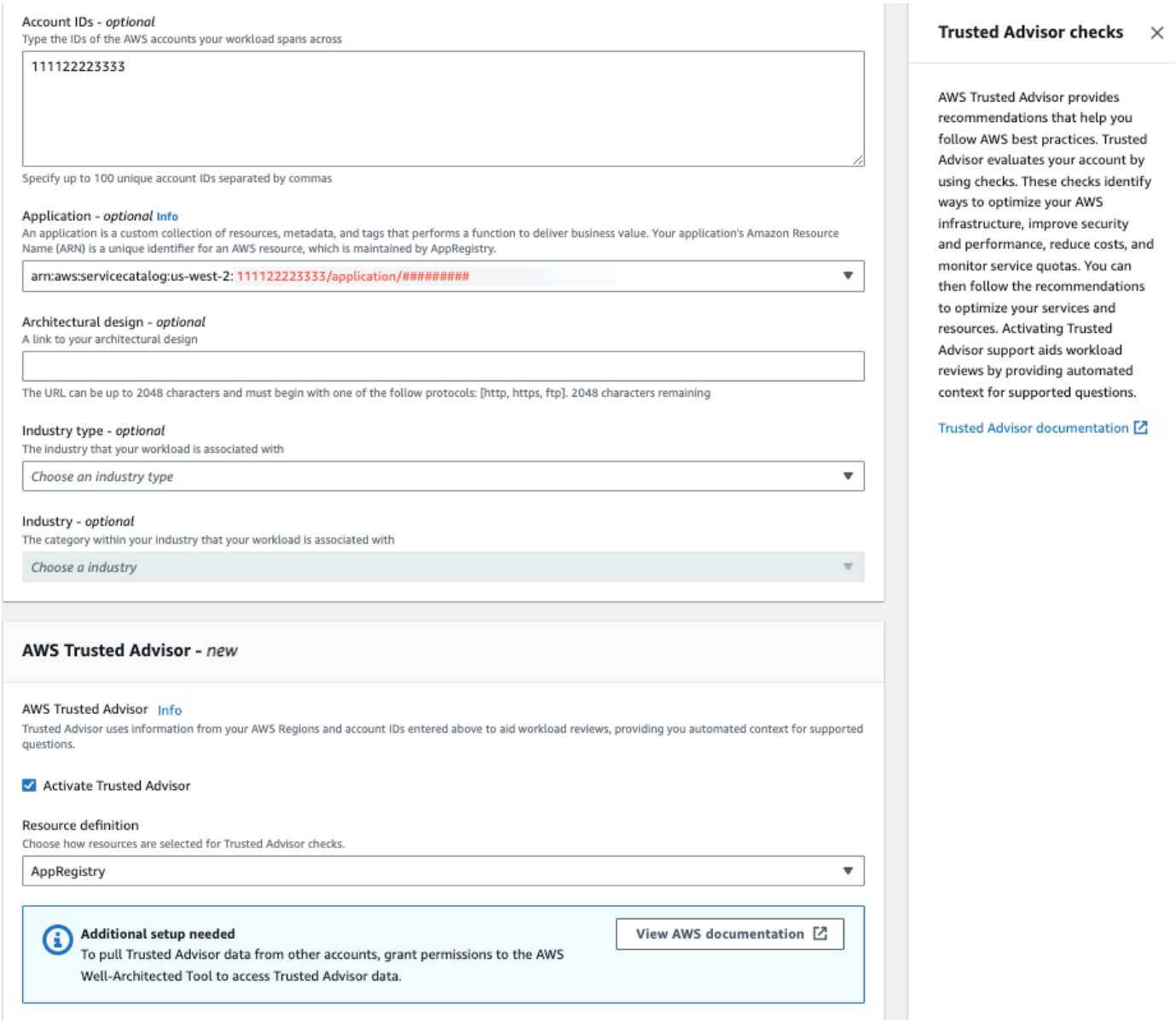
Ativar o AWS Trusted Advisor para uma workload

Opcionalmente, você pode integrar o AWS Trusted Advisor e ativá-lo por workload para clientes do AWS Business e Enterprise Support. Não há custo para integrar o Trusted Advisor ao AWS WA Tool, mas para obter detalhes sobre os preços do Trusted Advisor, consulte Planos de suporte da AWS. A ativação do Trusted Advisor para workloads pode oferecer uma abordagem mais abrangente,

automatizada e monitorada para revisar e otimizar workloads da AWS. Isso pode ajudar você a melhorar a confiabilidade, a segurança, o desempenho e a otimização de custos das workloads.

Para ativar o Trusted Advisor para uma workload

1. Para ativar o Trusted Advisor, os proprietários da workload podem usar o AWS WA Tool para atualizar uma workload existente ou criar uma nova workload selecionando Definir carga de trabalho.
2. Digite um ID de conta usado pelo Trusted Advisor no campo IDs de conta, selecione um ARN de aplicativo no campo Aplicativo ou ambos para ativar o Trusted Advisor.
3. Na seção AWS Trusted Advisor, selecione Ativar o Trusted Advisor.



4. Uma notificação de que o perfil de serviço do IAM será criado é exibida na primeira vez em que o Trusted Advisor for ativado para uma workload. A escolha Visualizar permissões exibe as permissões do perfil do IAM. Você pode ver o Nome da função, bem como as Permissões e as Relações de confiança que o JSON criou automaticamente para você no IAM. Depois que a função é criada, para workloads subsequentes que ativam o Trusted Advisor, somente a notificação para Configuração adicional necessária é mostrada.
5. No menu suspenso Definição de recurso, você pode selecionar Metadados da workload, AppRegistry ou Todos. A seleção de Definição de recursos define quais dados o AWS WA Tool obtém do Trusted Advisor para fornecer as verificações de status na avalição da workload que mapeiam as práticas recomendadas do Well-Architected.

   Metadados da workload: a workload é definida por IDs de conta e Regiões da AWS especificadas na workload.

   AppRegistry: a workload é definida por recursos (como pilhas do AWS CloudFormation) que estão presentes no aplicativo AppRegistry associado à workload.

   Tudo: a workload é definida pelos metadados da workload e pelos recursos do AppRegistry.
6. Escolha Próximo.
7. Aplique o AWSWell-Architected Framework à sua workload e escolha Definir carga de trabalho. As verificações do Trusted Advisor são vinculadas apenas ao AWS Well-Architected Framework e não a outras lentes.

O AWS WA Tool obtém periodicamente dados do Trusted Advisor usando os perfis criados no IAM. A perfil do IAM é criada automaticamente para o proprietário da workload. No entanto, para visualizar as informações do Trusted Advisor, os proprietários de quaisquer contas associadas na workload devem acessar o IAM e criar uma função; consulte ??? para obter mais detalhes. Se essa função não existir, o AWS WA Tool não poderá obter informações do Trusted Advisor para essa conta e exibirá um erro.

Para obter mais informações sobre como criar um perfil no AWS Identity and Access Management (IAM), consulte Criar uma função para um serviço da AWS (console) no Guia do usuário do IAM.

Ativar o Trusted Advisor para uma workload no IAM

> **Note**
>
> Os proprietários da workload devem ativar o suporte do Discovery para sua conta antes de criar uma workload do Trusted Advisor. A escolha de ativar o suporte do Discovery cria a função necessária para o proprietário da workload. Use as etapas a seguir para todas as outras contas associadas.

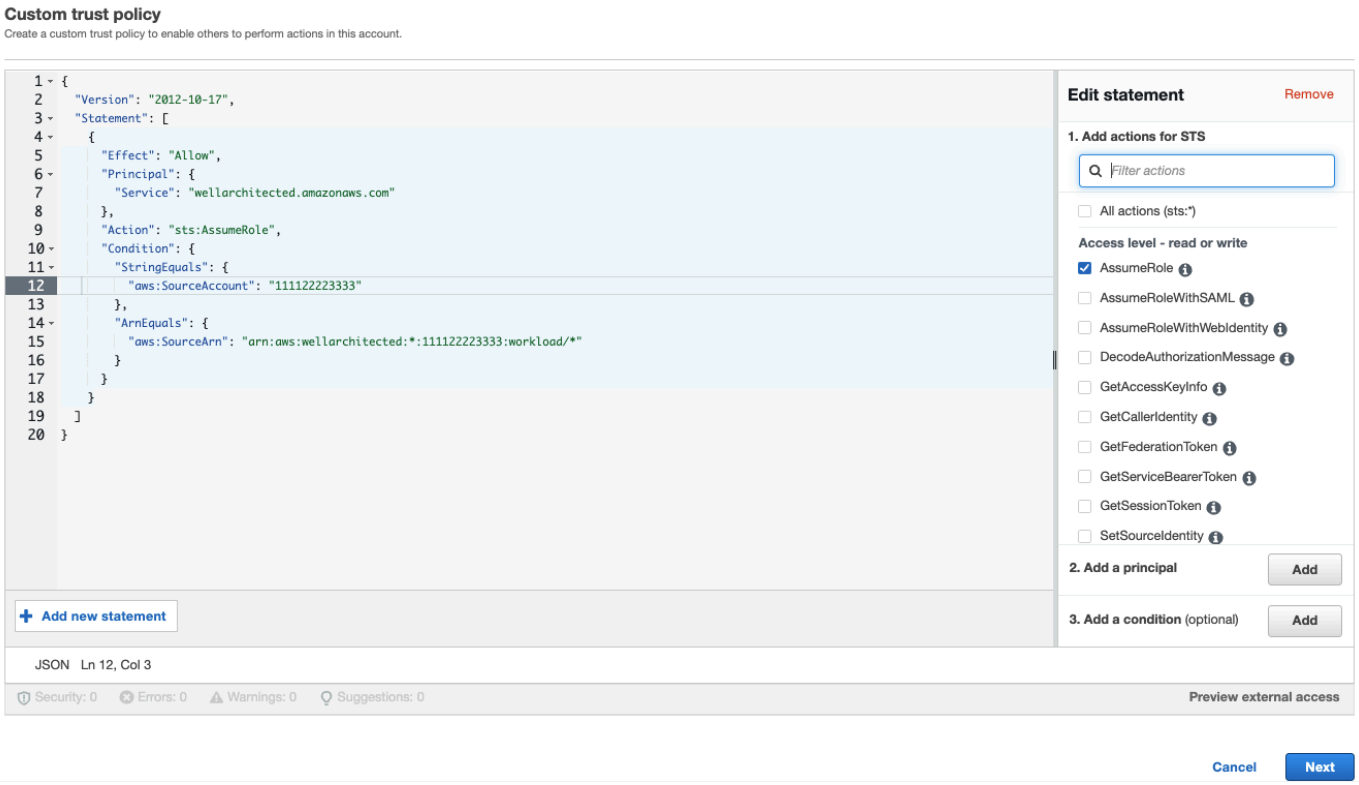
Os proprietários de contas associadas para workloads que ativaram o Trusted Advisor devem criar uma função no IAM para ver as informações do Trusted Advisor no AWS Well-Architected Tool.

Para criar uma função no IAM para que o AWS WA Tool obtenha informações do Trusted Advisor

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Perfis e, em seguida, Criar perfil.
3. Em Tipo de entidade confiável, escolha Política de confiança personalizada.
4. Copie e cole a seguinte Política de confiança personalizada no campo JSON no console do IAM, conforme mostrado na imagem a seguir. Substitua*WORKLOAD_OWNER_ACCOUNT_ID* com o ID da conta do proprietário da workload e selecione Próximo.

```
{
  "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

O `aws:sourceArn` no bloco de condições da política de confiança personalizada anterior é `"arn:aws:wellarchitected:*:`*`WORKLOAD_OWNER_ACCOUNT_ID`*`:workload/*"`, que é uma condição genérica que declara que essa função pode ser usada pelo AWS WA Tool para todas as workloads do proprietário da workload. No entanto, o acesso pode ser restringido a um ARN de workload específico ou a um conjunto de ARNs de workload. Para especificar vários ARNs, consulte a política de confiança exemplificada a seguir.

```
{
    "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. Na página Adicionar permissões, em Políticas de permissões, escolha Criar política para dar acesso ao AWS WA Tool à leitura de dados do Trusted Advisor. Selecionar Criar política abre uma nova janela.

> **Note**
>
> Além disso, você tem a opção de pular a criação das permissões durante a criação da função e criar uma política embutida após criar a função. Escolha Exibir função na mensagem de criação bem-sucedida da função e selecione Criar política embutida no menu suspenso Adicionar permissões na guia Permissões.

6. Copie e cole o seguinte JSON na janela do editor de política de permissões. No `Resource` ARN, *YOUR_ACCOUNT_ID*substitua pelo ID da sua própria conta, especifique a Região ou um asterisco (*) e escolha Próximo:Tags.

   Para obter detalhes sobre formatos de ARN, consulte Nome do recurso da Amazon (ARN) no Guia de referência da 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. Se o Trusted Advisor for ativado para uma workload e a Definição de Recurso for definida como AppRegistry ou Todos, todas as contas que possuem um recurso no aplicativo AppRegistry anexado à workload deverão adicionar a seguinte permissão à política de Permissões da função do Trusted Advisor.

```
{
    "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. (Opcional) Adicione tags. Escolha Próximo: revisar.
9. Revise a política, dê um nome a ela e selecione Criar política.
10. Na página Adicionar permissões para a função, selecione o nome da política que você acabou de criar e selecione Próximo.
11. Insira o nome da função, que deve usar a seguinte sintaxe: `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* e escolha Criar função. Substitua *`WORKLOAD_OWNER_ACCOUNT_ID`* pela ID da conta do proprietário da workload.

    Você deverá receber uma mensagem de sucesso na parte superior da página, notificando-o de que a função foi criada.
12. Para visualizar a função e a política de permissões associada, no painel de navegação esquerdo, em Gerenciamento de acesso, selecione Funções e pesquise o nome `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*. Selecione o nome da função para verificar se as relações de Permissões e Confiança estão corretas.

Desativar o Trusted Advisor para uma workload

Para ativar o Trusted Advisor para uma workload

Você pode desativar o Trusted Advisor para qualquer workload do AWS Well-Architected Tool editando sua workload e desmarcando Ativar o Trusted Advisor. Para obter mais informações sobre a edição de workloads, consulte the section called “Editar uma workload”.

Desativar o Trusted Advisor do AWS WA Tool não exclui os perfis criados no IAM. A exclusão de perfis do IAM exige uma medida de limpeza separada. Os proprietários da workload ou os proprietários das contas associadas devem excluir os perfis do IAM criados quando o Trusted Advisor for desativado no AWS WA Tool ou para impedir que o AWS WA Tool colete dados do Trusted Advisor para a workload.

Para excluir o **`WellArchitectedRoleForTrustedAdvisor`** no IAM

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

2. No painel de navegação do console do IAM, escolha Perfis.
3. Pesquise `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* e selecione o nome do perfil.
4. Escolha Excluir. Na janela pop-up, digite o nome do perfil para confirmar a exclusão e selecione Excluir novamente.

Para obter mais informações sobre como excluir um perfil do IAM, consulte Exclusão de uma função do IAM (console) no Guia do usuário do IAM.

Definir uma workload no AWS WA Tool

Workload é um conjunto de componentes que oferecem valor comercial. Por exemplo, workloads podem ser sites de marketing, sites de comércio eletrônico, o backend de um aplicativo móvel e plataformas de analytics. A definição precisa de uma workload ajuda a garantir uma análise abrangente dos pilares do AWS Well-Architected Framework.

Como definir uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. Se esta for a primeira vez que você usa o AWS WA Tool, você verá uma página com os recursos do serviço. Na seção Define a workload (Definir uma carga de trabalho), selecione Define workload (Definir carga de trabalho).

   Como alternativa, no painel de navegação à esquerda, selecione Workloads (Cargas de trabalho) e selecione Define workload (Definir carga de trabalho).

   Para obter detalhes sobre como a AWS usa seus dados de workload, selecione Por que a AWS precisa desses dados e como eles serão usados?
3. Na caixa Name (Nome), insira um nome para a carga de trabalho.

> **Note**
>
> O nome deve ter de 3 a 100 caracteres. Pelo menos três caracteres não devem ser espaços. Os nomes da carga de trabalho devem ser exclusivos. Os espaços e a capitalização são ignorados ao verificar a exclusividade.

4. Na caixa Description (Descrição), insira uma descrição da carga de trabalho. A descrição deve ter de 3 a 250 caracteres.
5. Na caixa Review owner (Proprietário da revisão) insira o nome, o endereço de e-mail ou o identificador do grupo principal ou do indivíduo proprietário do processo de revisão da carga de trabalho.
6. Na caixa Environment (Ambiente), escolha o ambiente para a carga de trabalho:
   - Produção: a workload é executada em um ambiente de produção.
   - Pré-produção: a workload é executada em um ambiente de pré-produção.
7. Na seção Regions (Regiões), escolha as regiões para a carga de trabalho:
   - Regiões da AWS: escolha as Regiões da AWS onde sua workload é executada, uma de cada vez.
   - Regiões que não são da AWS: insira os nomes das regiões fora da AWS onde a workload é executada. Você pode especificar até cinco regiões exclusivas, separadas por vírgulas.

   Use as duas opções se isso for apropriado para a carga de trabalho.
8. (Opcional) Na caixa IDs da conta, insira os IDs das Contas da AWS associadas à workload. Você pode especificar até 100 IDs de conta exclusivos, separados por vírgulas.

   Se o Trusted Advisor estiver ativado, todos os IDs de conta especificados serão usados para obter dados do Trusted Advisor. Consulte Ativação do AWS Trusted Advisor para obter uma workload para conceder permissões ao AWS WA Tool para obter dados do Trusted Advisor em seu nome no IAM.
9. (Opcional) Na caixa Aplicativo, insira o ARN do aplicativo AWS Service Catalog AppRegistry que você deseja associar a essa workload. Somente um ARN pode ser especificado por workload, e o aplicativo e a workload devem estar na mesma região.
10. (Opcional) Na caixa Architectural design (Design de arquitetura) insira o URL do seu projeto de arquitetura.
11. (Opcional) Na caixa Industry type (Tipo de setor), escolha o tipo de setor associado à carga de trabalho.
12. (Opcional) Na caixa Industry (Setor), escolha o setor que melhor corresponde à carga de trabalho.
13. (Opcional) Na Trusted Advisor seção, para ativar as verificações Trusted Advisor de sua workload, selecione Ativar o Trusted Advisor. Pode ser necessária uma configuração adicional para as contas associadas à sua workload. Consulte the section called “Ativação do Trusted Advisor” para conceder permissões ao AWS WA Tool para obter dados do Trusted Advisor em

seu nome. Selecione entre Workload Metadata, AppRegistry ou All em Definição de recurso para definir quais recursos o AWS WA Tool usa para executar verificações do Trusted Advisor.

14. (Opcional) Na seção Jira, para ativar as configurações de sincronização do Jira em nível de workload para a workload, selecione Substituir as configurações no nível da conta. Pode ser necessária uma configuração adicional para as contas associadas à sua workload. Consulte AWS Well-Architected Tool Conector for Jira para começar a instalar e configurar o conector. Selecione entre Não sincronizar workload, Sincronizar workload - Manual e Sincronizar workload - Automático e, opcionalmente, insira uma chave de projeto do Jira para sincronizar.

> **Note**
>
> Se você não substituir as configurações no nível da conta, as workloads usarão como padrão a configuração de sincronização do Jira no nível da conta.

15. (Opcional) Na seção Tags, adicione as tags que você deseja associar à workload.

    Para obter mais informações sobre tags, consulte Marcando seus Recursos AWS WA Tool.

16. Escolha Próximo.

    Se uma caixa obrigatória estiver em branco ou se um valor especificado não for válido, você deverá corrigir o problema para poder continuar.

17. (Opcional) Na etapa Aplicar Perfil, associe um perfil à workload selecionando um perfil existente, pesquisando o nome do perfil ou escolhendo Criar perfil para criar um perfil. Escolha Próximo.

18. Escolha as perspectivas que se aplicam a esta carga de trabalho. Até 20 lentes podem ser adicionadas a uma workload. Para obter descrições das lentes oficiais da AWS, consulte Lentes.

    As lentes podem ser selecionadas em Lentes personalizadas (lentes que você criou ou que foram compartilhadas com sua Conta da AWS), Catálogo de lentes (lentes oficiais da AWS disponíveis para todos os usuários) ou ambas.

> **Note**
>
> A seção Lentes personalizadas estará vazia se você não tiver criado uma lente personalizada ou tiver uma lente personalizada compartilhada com você.

> **Isenção de responsabilidade**
>
> Ao acessar e/ou aplicar lentes personalizadas criadas por outro usuário ou conta da AWS, você reconhece que as lentes personalizadas criadas por outros usuários e compartilhadas com você são Conteúdo de Terceiros, conforme definido no Contrato do Cliente da AWS.

19. Selecione Define workload (Definir carga de trabalho).

    Se uma caixa obrigatória ficar em branco, ou se um valor especificado não for válido, será necessário corrigir o problema antes de definir a carga de trabalho.

Documentar uma workload no AWS WA Tool

Depois de definir uma workload no AWS Well-Architected Tool, você pode documentar o respectivo estado abrindo a página Analisar carga de trabalho. Isso ajuda você a avaliar a workload e acompanhar seu progresso ao longo do tempo.

Como documentar o estado de uma carga de trabalho

1. Depois de definir a carga de trabalho, você verá uma página com os detalhes atuais da carga de trabalho. Escolha Start reviewing (Iniciar a revisão) para começar.

   Como alternativa, no painel de navegação à esquerda, selecione Workloads (Cargas de trabalho) e o nome da carga de trabalho para abrir a página de detalhes da carga de trabalho. Escolha Continue reviewing (Continuar a revisão).

   (Opcional) Se um perfil estiver associado à sua workload, o painel de navegação esquerdo conterá uma lista de perguntas de revisão da workload priorizada que você pode usar para acelerar o processo de análise da workload.
2. Agora é apresentada a primeira pergunta. Para cada pergunta:

   a. Leia a pergunta e determine se ela se aplica à carga de trabalho.

      Para obter mais instruções, escolha Info e visualize as informações no painel à direita.

      - Se a pergunta não se aplicar à carga de trabalho, selecione Question does not apply to this workload (A pergunta não se aplica a esta carga de trabalho).

- Caso contrário, selecione na lista as melhores práticas que você está seguindo no momento.

  Se não estiver seguindo nenhuma das melhores práticas no momento, selecione None of these (Nenhuma das opções).

Para obter mais instruções sobre qualquer item, selecione Info e visualize as informações no painel à direita.

b. (Opcional) Se uma ou mais práticas recomendadas não se aplicarem à sua workload, escolha Marcar as melhores práticas que não se aplicam a essa workload e selecione-as. Para cada melhor prática selecionada, você pode, opcionalmente, selecionar um motivo e fornecer detalhes adicionais.

c. (Opcional) Use a caixa Notes (Notas) para registrar informações relacionadas à pergunta.

   Por exemplo, é possível descrever por que a pergunta não se aplica ou fornecer detalhes adicionais sobre as melhores práticas selecionadas.

d. Selecione Next (Próximo) para prosseguir para a próxima pergunta.

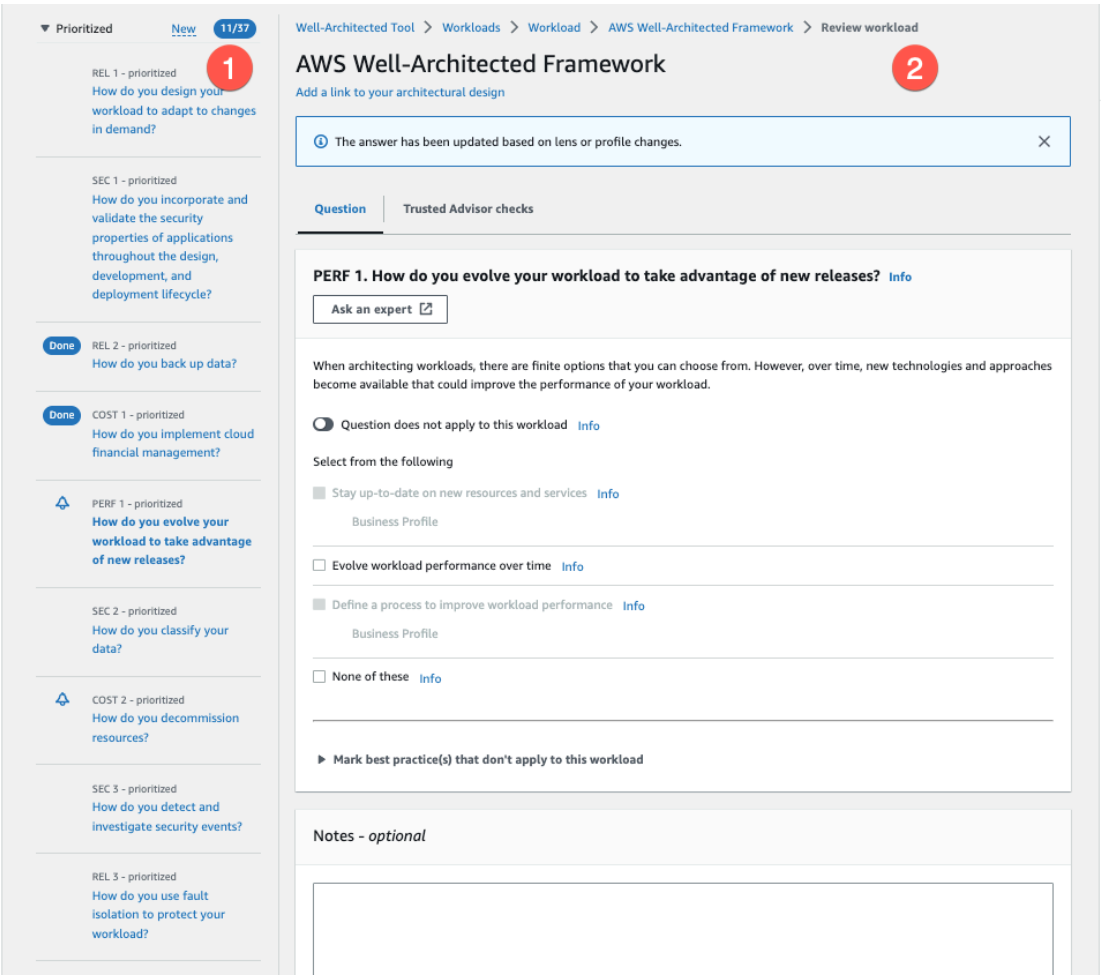
Repita essas etapas para cada pergunta em cada pilar.

3. Escolha Save and exit (Salvar e sair) a qualquer momento para salvar as alterações e interromper a documentação da carga de trabalho.

Depois de documentar sua workload, você pode retornar as qualquer momento às perguntas para continuar a revisá-la. Para ter mais informações, consulte Reviewing a workload with AWS Well-Architected Framework.

Analisar uma workload com o AWS Well-Architected Framework

Você pode analisar a workload no console na página Analisar carga de trabalho. Essa página apresenta práticas recomendadas e recursos úteis para o desempenho da workload.



1. Para abrir a página Analisar carga de trabalho, na página de detalhes da workload, escolha Continuar analisando. O painel de navegação esquerdo mostra as perguntas de cada pilar. As perguntas que você respondeu estão marcadas como Concluídas. O número de perguntas respondidas em cada pilar é mostrado ao lado do nome do pilar.

   Você pode navegar para perguntas em outros pilares selecionando o nome do pilar e escolhendo a pergunta que deseja responder.

   (Opcional) Se um perfil estiver associado à sua workload, AWS WA Tool usa as informações do perfil para determinar quais perguntas na análise da workload são priorizadas e quais perguntas não são aplicáveis à sua empresa. No painel de navegação esquerdo, você pode usar as perguntas priorizadas para ajudar a acelerar o processo de avaliação da workload. Um ícone de notificação aparece ao lado das perguntas recém-adicionadas à lista de perguntas priorizadas.
2. O painel do meio exibe a pergunta atual. Selecione as práticas recomendadas que você está seguindo. Selecione Info (Informações) para obter informações adicionais sobre a pergunta ou sobre uma prática recomendada. Escolha Pergunte a um especialista para acessar a comunidade

AWS re:Post dedicada ao AWS Well-Architected. O AWS re:Post é um substituto da comunidade de perguntas e respostas baseado em tópicos para fóruns da AWS. Com o re:Post, você pode encontrar respostas, responder a perguntas, participar de um grupo, seguir tópicos populares e votar em suas perguntas e respostas favoritas.

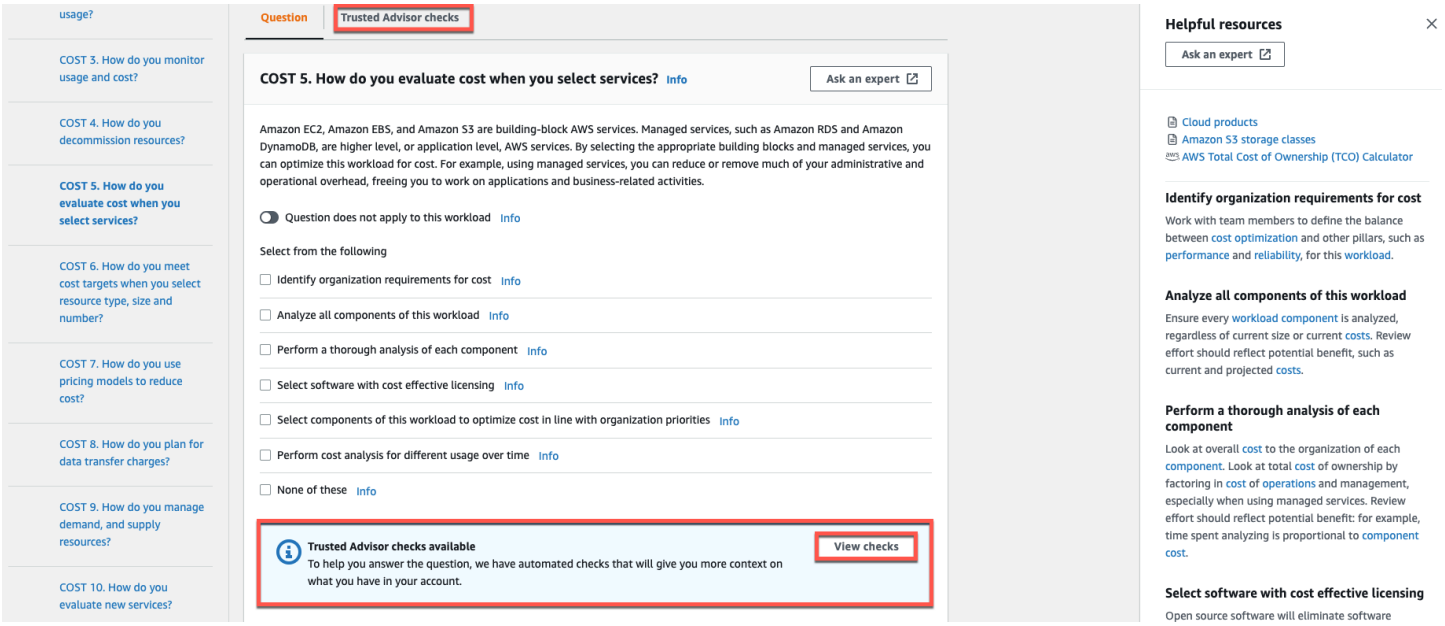
(Opcional) Para marcar uma ou mais práticas recomendadas como não aplicáveis, selecione Marcar prática(s) recomendada(s) que não se aplicam a esta workload e selecione-as.

Use os botões na parte inferior desse painel para ir para a próxima pergunta, retornar à pergunta anterior ou salvar suas alterações e sair.

3. O painel de ajuda à direita exibe informações adicionais e recursos úteis. Escolha Pergunte a um especialista para acessar a comunidade do AWS re:Post dedicada ao AWS Well-Architected. Nessa comunidade, você pode fazer perguntas relacionadas ao projeto, à criação, à implantação e à operação de workloads na AWS.

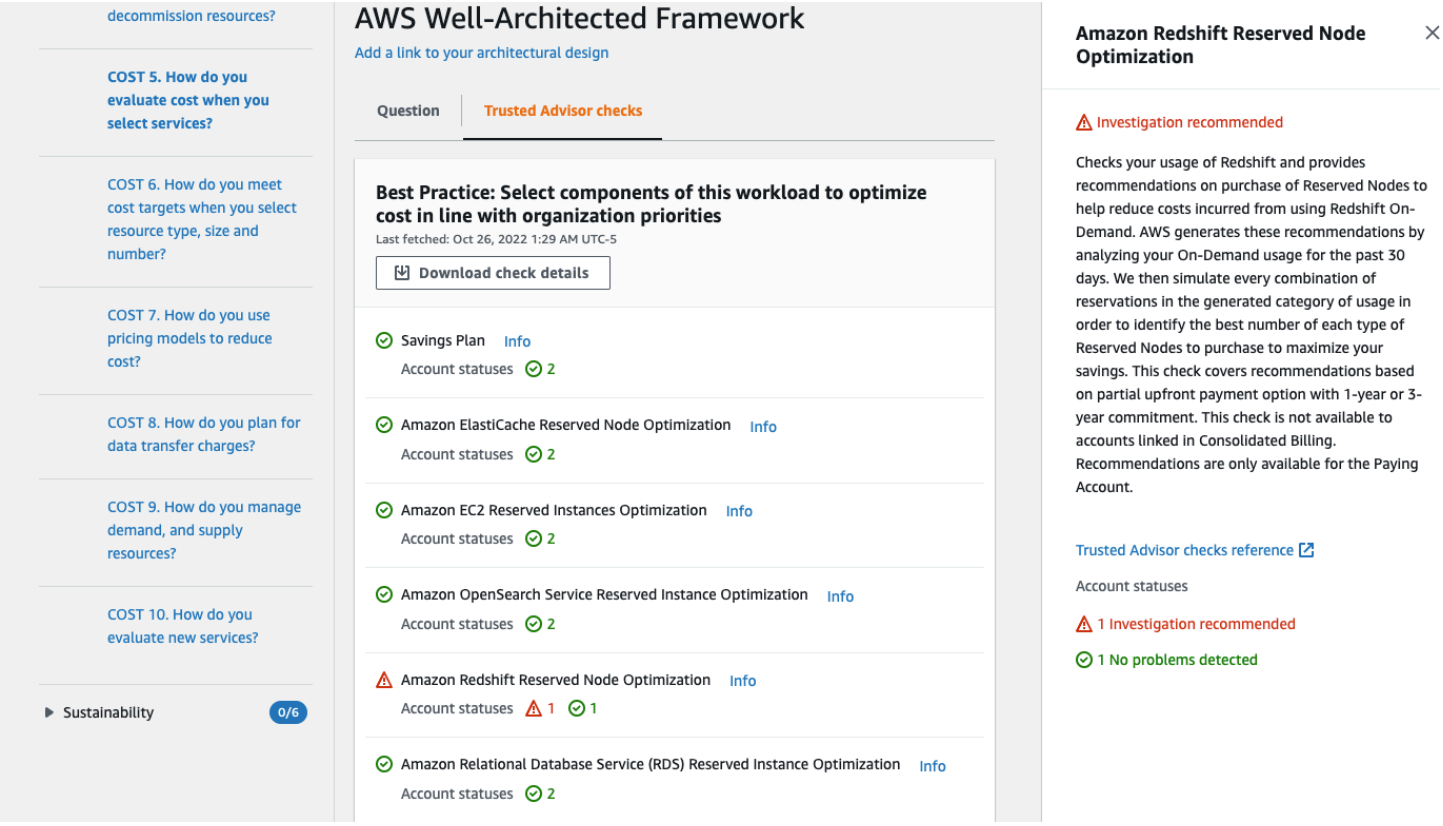
Visualizar verificações do Trusted Advisor de sua workload

Se o Trusted Advisor estiver ativado para sua workload, uma guia de Verificações do Trusted Advisor será exibida ao lado da Pergunta. Se houver alguma verificação disponível para a melhor prática, uma notificação de que há verificações Trusted Advisor disponíveis será exibida após a seleção da pergunta. Selecionar Exibir verificações leva você para a guia de verificações Trusted Advisor.



Na guia Verificações do Trusted Advisor, você pode ver informações mais detalhadas sobre as verificações de melhores práticasTrusted Advisor, ver links para a Trusted Advisor documentação

no painel Recursos de ajuda ou Baixar detalhes da verificação, que fornece um relatório das Trusted Advisor verificações e status de cada prática recomendada em um arquivo CSV.



As categorias de cheques do Trusted Advisor são exibidas como ícones coloridos, e o número ao lado de cada ícone mostra o número de contas nesse status.

- Ação recomendada (vermelho) - o Trusted Advisor recomenda uma ação para a verificação.
- Investigação recomendada (amarelo): Trusted Advisordetecta um possível problema para a verificação.
- Nenhum problema detectado (verde) - o Trusted Advisor não detecta um problema para a verificação.
- Itens excluídos (cinza): o número de verificações que excluíram itens, como recursos que você deseja que uma verificação ignore.

Para obter mais informações sobre as verificações Trusted Advisor fornecidas, consulte Exibir categorias de verificação no Guia Suporte do usuário.

Selecionar o link Informações ao lado de cada verificação Trusted Advisor exibe informações sobre a verificação no painel Recursos de ajuda. Para obter mais informações, consulte a AWS Trusted Advisor check reference no Guia do usuário do Suporte.

Salvar um marco referente a uma workload no AWS WA Tool

Você pode salvar um marco referente a uma workload a qualquer momento. Um marco registra o estado atual da carga de trabalho.

Como salvar um marco

1. Na página de detalhes da carga de trabalho, selecione Save milestone (Salvar marco).
2. Na caixa Milestone name (Nome do marco), insira um nome para o marco.

   > **Note**
   >
   > O nome deve ter de 3 a 100 caracteres. Pelo menos três caracteres não devem ser espaços. Os nomes de marcos associados a uma carga de trabalho devem ser exclusivos. Os espaços e a capitalização são ignorados ao verificar a exclusividade.

3. Escolha Salvar.

Depois que um marco for salvo, não será possível alterar os dados da workload capturados naquele marco.

Para ter mais informações, consulte Marcos.

Tutorial: documentar uma workload do AWS Well-Architected Tool

Este tutorial descreve o uso do AWS Well-Architected Tool para documentar e medir uma carga de trabalho. Este exemplo ilustra, passo a passo, como definir e documentar uma carga de trabalho para um site de comércio eletrônico de varejo.

Tópicos

- Etapa 1: definir uma workload
- Etapa 2: documentar o estado da workload
- Etapa 3: Revisar o plano de aprimoramento
- Etapa 4: Faça melhorias e avalie o progresso

Etapa 1: definir uma workload

Comece definindo uma carga de trabalho. Há duas maneiras de definir uma workload. Neste tutorial, não estamos definindo uma workload com base em um modelo de avaliação. Para obter mais detalhes sobre como definir uma workload com base em um modelo de avaliação, consulte the section called “Definir uma workload”.

Como definir uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.

   > **Note**
   >
   > O usuário que documenta o estado da workload deve ter permissões de acesso total ao AWS WA Tool.

2. Na seção Define a workload (Definir uma carga de trabalho), selecione Define workload (Definir carga de trabalho).
3. Na caixa Name (Nome), insira **`Retail Website - North America`** como o nome da carga de trabalho.
4. Na caixa Description (Descrição), insira uma descrição para a carga de trabalho.

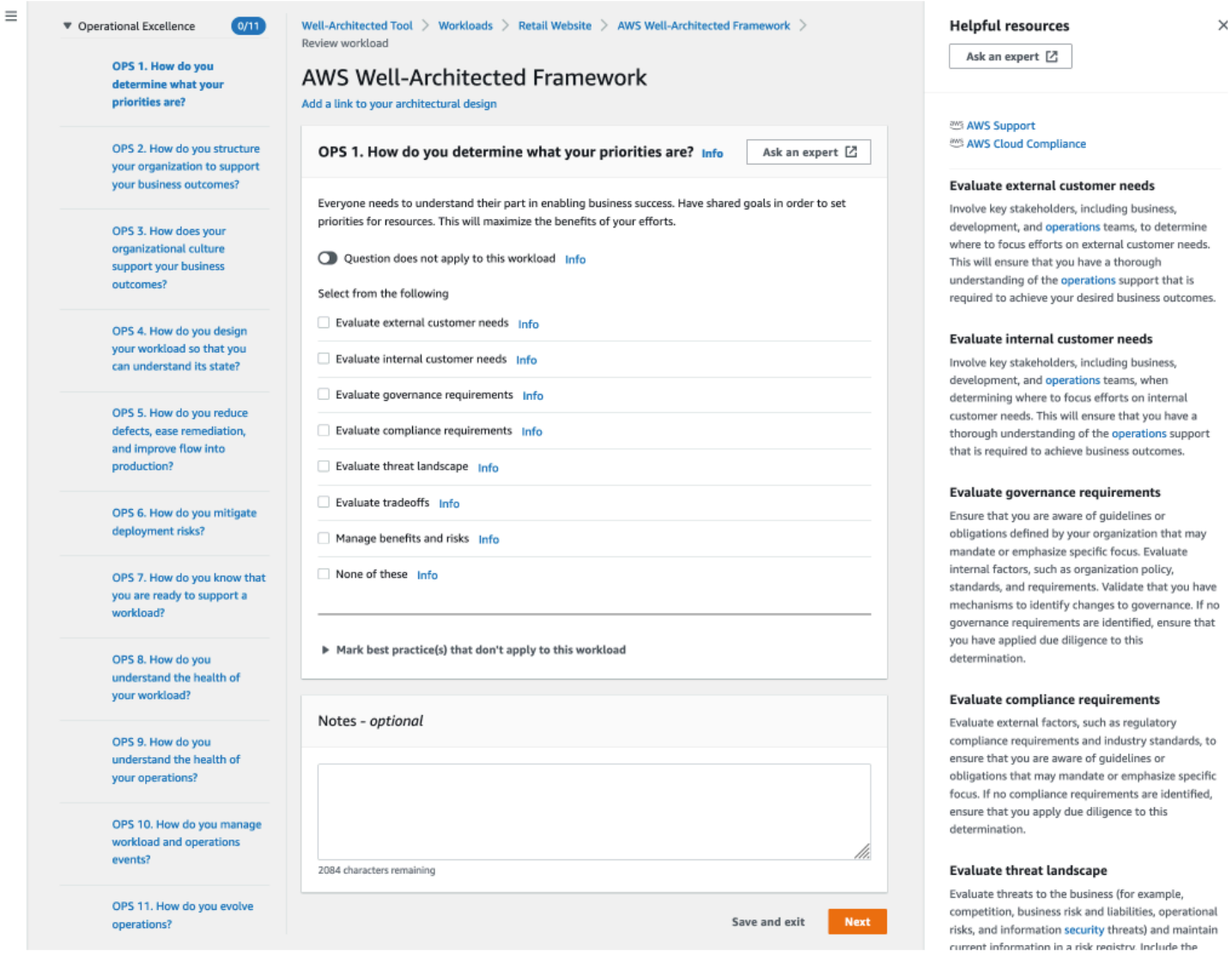
5. Na caixa Proprietário da revisão inserimos o nome da pessoa responsável pelo processo de revisão da workload.
6. Na caixa Ambiente, indicamos que a workload está em um ambiente de produção.
7. Nossa workload é executada tanto na AWS como em nosso data center local:
    a. Escolha Regiões da AWS e selecione as duas regiões na América do Norte onde a workload é executada.
    b. Selecione também Regiões que não são da AWS e insira um nome para o data center local.
8. A caixa IDs de conta é opcional. Não associe quaisquer Contas da AWS a essa workload.
9. A caixa Aplicativo é opcional. Não insira um ARN da aplicação para essa workload.
10. A caixa Diagrama de arquitetura é opcional. Não associe um diagrama de arquitetura a essa workload.
11. As caixas Industry type (Tipo de setor) e Industry (Setor) são opcionais e não são especificadas para essa carga de trabalho.
12. A seção Trusted Advisor é opcional. Não opte por Ativar o suporte ao Trusted Advisor para essa workload.
13. A seção Jira é opcional. Não opte por Substituir as configurações do nível da conta na seção Jira referente a essa workload.
14. Neste exemplo, não aplique nenhuma tag à workload. Escolha Próximo.
15. A etapa Aplicar perfil é opcional. Não aplique um perfil a essa workload. Escolha Próximo.
16. Nesse exemplo, aplique as Lentes do AWS Well-Architected Framework, que são selecionadas automaticamente. Selecionamos Define workload (Definir carga de trabalho) para salvar esses valores e definir a carga de trabalho.
17. Depois que a carga de trabalho for definida, escolha Start reviewing (Iniciar a revisão) para começar a documentar o estado da carga de trabalho.

Etapa 2: documentar o estado da workload

Para documentar o estado da workload, são apresentadas perguntas para as lentes selecionadas que abrangem os pilares do AWS Well-Architected Framework: excelência operacional, segurança, confiabilidade, eficiência de desempenho, otimização de custos e sustentabilidade.

Para cada pergunta, escolha as melhores práticas que você está seguindo na lista fornecida. Se precisar de detalhes sobre uma prática recomendada, selecione Info (Informações) e visualize os recursos e as informações adicionais no painel à direita.

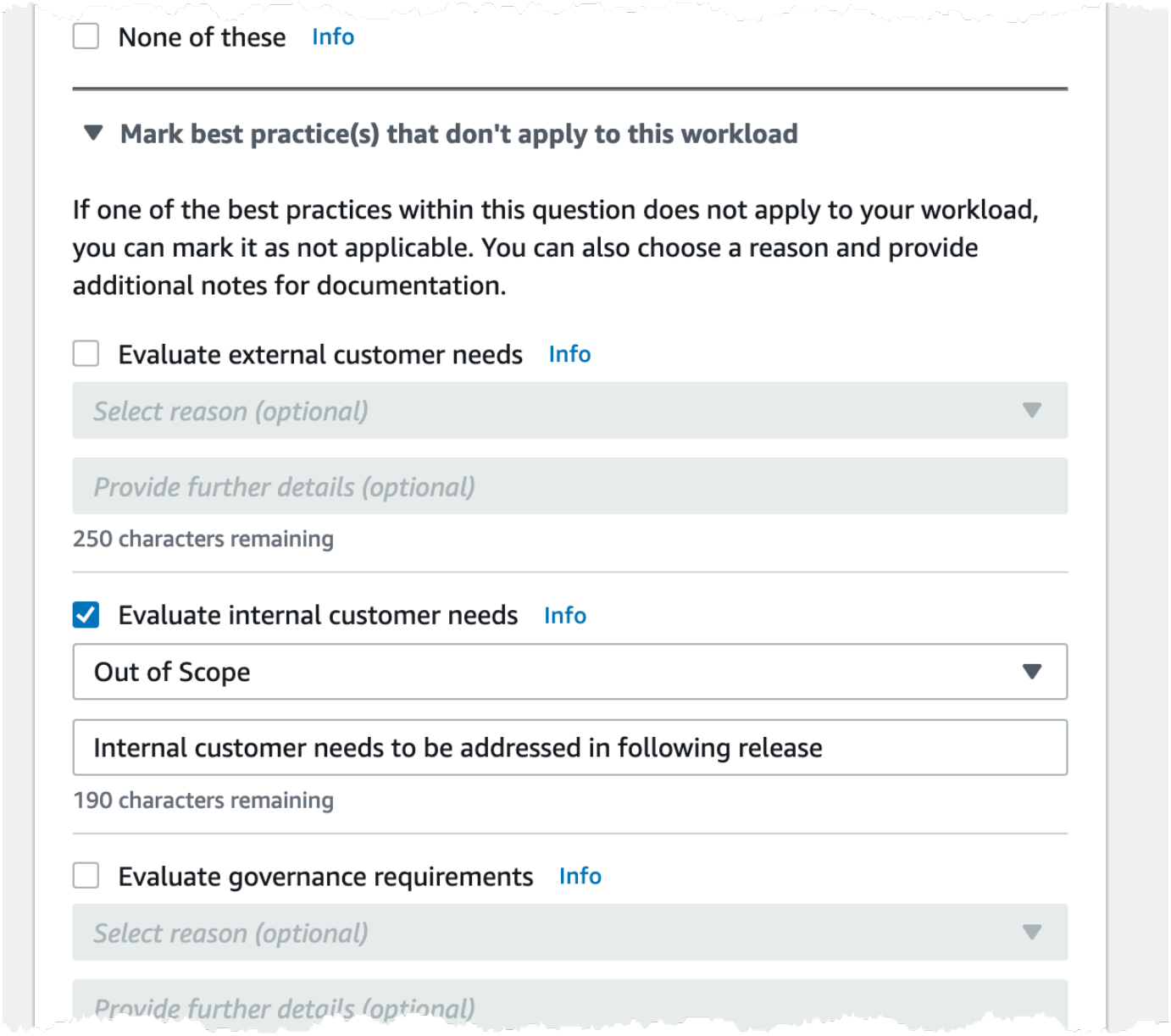
Escolha Pergunte a um especialista para acessar a comunidade do AWS re:Post dedicada ao AWS Well-Architected. Nessa comunidade, você pode fazer perguntas relacionadas ao projeto, à criação, à implantação e à operação de workloads na AWS.



1. Escolha Next (Próximo) para prosseguir para a próxima pergunta. Você pode usar o painel à esquerda para navegar até uma pergunta diferente do mesmo pilar ou até uma pergunta em um outro pilar.
2. Se selecionar A pergunta não se aplica a esta workload ou Nenhuma das opções, a AWS recomenda que você inclua o motivo na caixa Notas. Essas notas são incluídas como parte do

relatório de carga de trabalho e poderão ser úteis no futuro, conforme forem feitas alterações na carga de trabalho.

> **Note**
>
> Opcionalmente, você pode marcar uma ou mais práticas recomendadas individuais como não aplicáveis. Escolha Marcar as práticas recomendadas que não se aplicam a essa workload e selecione as práticas recomendadas que não se aplicam. Para cada melhor prática selecionada, você pode, opcionalmente, selecionar um motivo e fornecer detalhes adicionais. Repita o procedimento para cada prática recomendada que não se aplica.



> **Note**
>
> Você pode pausar esse processo a qualquer momento escolhendo Salvar e sair. Para continuar mais tarde, abra o console do AWS WA Tool e escolha Workloads no painel de navegação à esquerda.

3. Selecione o nome da carga de trabalho para abrir a página de detalhes da carga de trabalho.
4. Escolha Continue reviewing (Continuar a revisão) e navegue até onde parou.

5. Depois de concluir todas as perguntas, uma página de visão geral da carga de trabalho será exibida. Você pode avaliar esses detalhes agora ou navegar até eles mais tarde selecionando Workloads (Cargas de trabalho) no painel de navegação à esquerda e selecionando o nome da carga de trabalho.

Depois de documentar o estado da carga de trabalho pela primeira vez, você deve salvar um marco e gerar um relatório de carga de trabalho.

Um marco captura o estado atual da carga de trabalho e permite medir o andamento à medida que são feitas alterações com base no seu plano de melhoria.

Na página de detalhes da workload:

1. Na seção Visão geral da workload, escolha o botão Salvar etapa.
2. Insira **`Version 1.0 - initial review`** como Nome da etapa.
3. Escolha Salvar.
4. Para gerar um relatório da carga de trabalho, selecione a perspectiva desejada, escolha Generate report (Gerar relatório) e um arquivo PDF será criado. Esse arquivo contém o estado da carga de trabalho, o número de riscos identificados e uma lista de melhorias sugeridas.

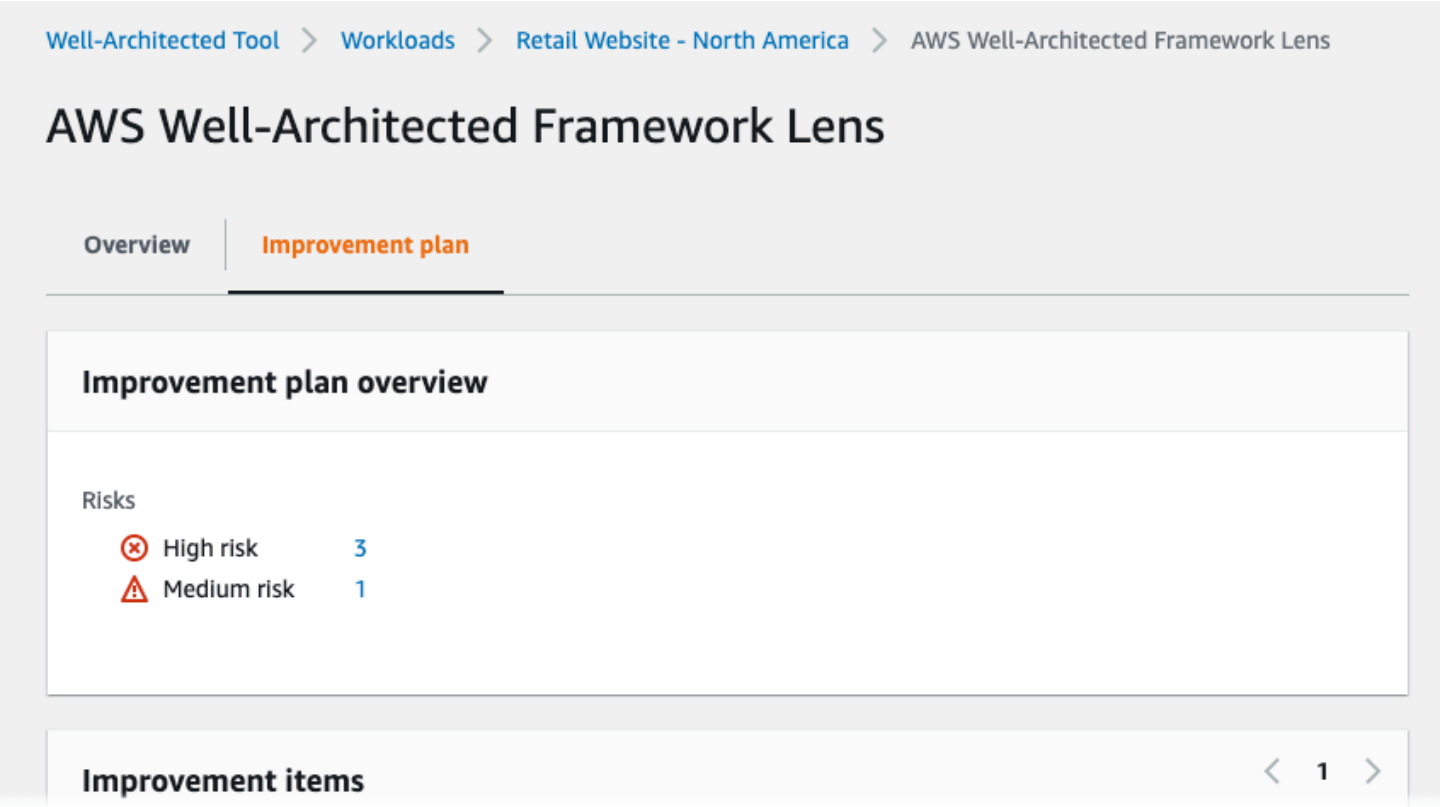
Etapa 3: Revisar o plano de aprimoramento

Com base nas melhores práticas selecionadas, o AWS WA Tool identifica áreas de alto e médio risco conforme medidas em relação à perspectiva do AWS Well-Architected Framework.

Revisar o plano de aprimoramento:

1. Para revisar o plano de melhoria, escolha AWS Well-Architected Framework na seção Lentes da página Visão geral.
2. Escolha Improvement plan (Plano de melhoria).

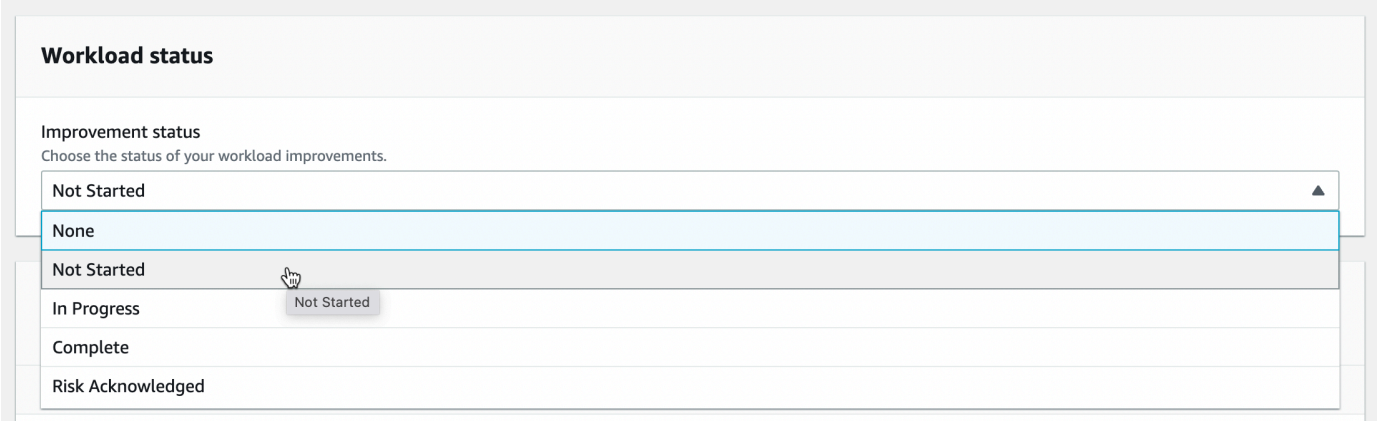
Para esse exemplo específico de workload, três problemas de alto risco e um problema de médio risco foram identificados pela perspectiva do AWS Well-Architected Framework.



Atualize o Status de melhoria da workload para indicar que melhorias na workload ainda não foram iniciadas.

Para alterar o Status de melhoria:

1. No plano de melhoria, clique no nome da workload (**`Retail Website - North America`**) nas navegações estruturais na parte superior da página.
2. Clique na guia Propriedades.
3. Acesse a seção Status da workload e selecione Não iniciada na lista suspensa.



4. Volte até o plano de melhoria na guia Propriedades clicando na guia Visão geral e no link AWS Well-Architected Framework na seção Lentes. Em seguida, clique na guia Plano de melhoria na parte superior da página.

A seção Improvement items (Itens de melhoria) mostra os itens de melhoria recomendados identificados na carga de trabalho. As perguntas são ordenadas com base na prioridade dos pilares definidos, com os problemas de risco alto listados primeiro, seguidos pelos problemas de risco médio.

Expanda Recommended improvement items (Itens de melhoria recomendados) para mostrar as melhores práticas para uma pergunta. Cada ação de melhoria recomendada é vinculada a uma instrução especializada detalhada para ajudar a eliminar ou ao menos mitigar os riscos identificados.

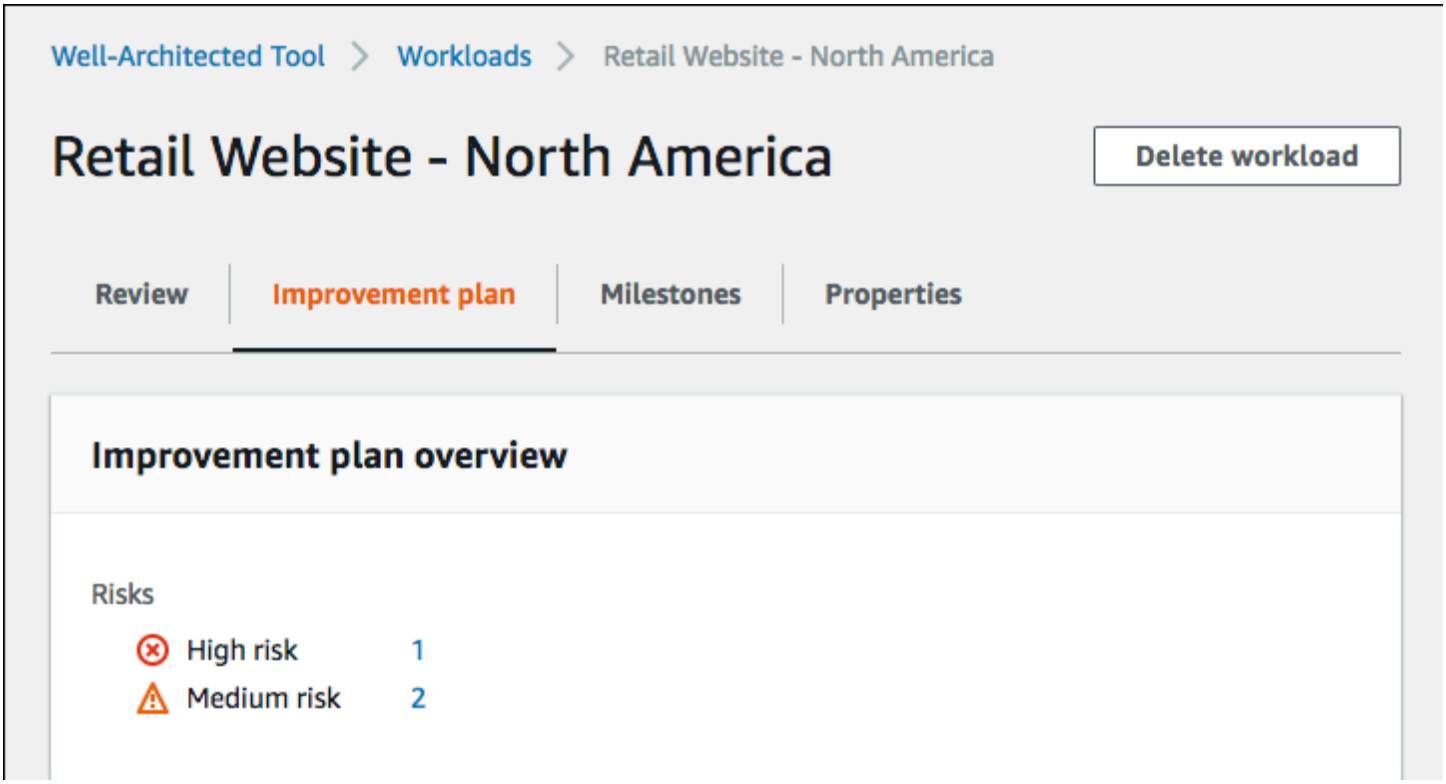
Se um perfil estiver associado à workload, uma contagem dos riscos priorizados será exibida na seção Visão geral do plano de melhoria, e você poderá filtrar a lista de Itens de melhoria selecionando Priorizado por perfil. A lista de itens de melhoria exibe um rótulo Priorizado.

Etapa 4: Faça melhorias e avalie o progresso

Como parte desse plano de melhoria, um dos problemas de alto risco foi resolvido com a adição de suporte do Amazon CloudWatch e do AWS Auto Scaling à workload.

Na seção Itens de aprimoramento:

1. Escolha a pergunta pertinente e atualize as práticas recomendadas selecionadas para refletir as alterações. As Notas são adicionadas para registrar as melhorias.
2. Depois, escolha Salvar e sair para atualizar o estado da workload.
3. Depois de fazer alterações, você pode retornar ao Improvement plan (Plano de melhoria) e ver o efeito dessas alterações na carga de trabalho. Nesse exemplo, essas ações melhoraram o perfil de risco reduzindo o número de problemas de alto risco de três para apenas um.



É possível salvar um marco nesse ponto e, depois, ir para Milestones (Marcos) para ver como a carga de trabalho melhorou.

Workloads

Uma workload é um conjunto de códigos e recursos que agrega valor empresarial, como uma aplicação voltada para o cliente ou um processo de back-end.

Uma workload pode consistir em um subconjunto de recursos em uma única Conta da AWS ou ser uma coleção de vários recursos que abrangem várias Contas da AWS. Uma pequena empresa pode ter apenas algumas cargas de trabalho, enquanto uma grande empresa pode ter milhares.

A página Workloads (Cargas de trabalho), disponível no painel de navegação à esquerda, fornece informações sobre as suas cargas de trabalho e todas as cargas de trabalho que foram compartilhadas com você.

As informações a seguir são exibidas para cada carga de trabalho:

Nome

O nome da carga de trabalho.

Proprietário

O ID da Conta da AWS que é proprietária da workload.

Perguntas respondidas

O número de perguntas respondidas.

Riscos altos

O número de problemas de alto risco (HRI – high risk issues) identificados.

Riscos médios

O número de problemas de risco médio (MRI – medium risk issues) identificados.

Status de melhoria

O status de melhoria que você definiu para a carga de trabalho:

- Nenhum
- Não iniciado
- Em andamento
- Concluído
- Risco reconhecido

Última atualização

Data e hora em que a carga de trabalho foi atualizada pela última vez.

Após escolher uma carga de trabalho na lista:

- Para revisar os detalhes da carga de trabalho, selecione View details (Visualizar detalhes).
- Para alterar as propriedades da carga de trabalho, selecione Edit (Editar).
- Para gerenciar o compartilhamento da workload com outras Contas da AWS, usuários, AWS Organizations ou unidades organizacionais (OUs), escolha Exibir detalhes e, em seguida, Compartilhamentos.
- Para excluir a carga de trabalho e todos os seus marcos, selecione Delete (Excluir). Somente o proprietário da carga de trabalho pode excluí-la.

> **Warning**
>
> A exclusão de uma workload não pode ser desfeita. Todos os dados associados à carga de trabalho serão excluídos.

Problemas de alto risco (HRI) e problemas de risco médio (MRI)

Os problemas de alto risco (HRIs) identificados no AWS Well-Architected Tool são escolhas arquitetônicas e operacionais que a AWS descobriu que podem resultar em um impacto negativo significativo para uma empresa. Esses HRI podem afetar ativos, indivíduos e operações organizacionais. Os problemas de risco médio (MRI) também podem afetar negativamente os negócios, mas em menor grau. Esses problemas são baseados em suas respostas no AWS Well-Architected Tool. As práticas recomendadas correspondentes são amplamente aplicadas pela AWS e pelos clientes da AWS. Essas práticas recomendadas são a orientação definida pela estrutura e pelas lentes da AWS Well-Architected.

> **Note**
>
> Essas são apenas diretrizes e os clientes devem avaliar e medir o impacto de não implementar as melhores práticas em seus negócios. Se houver motivos técnicos ou comerciais específicos que impeçam a aplicação de uma prática recomendada à workload, o risco poderá ser menor do que o indicado. O AWS sugere que os clientes documentem

esses motivos e como eles afetam as melhores práticas nas notas de workload. Para todos os HRIs e MRIs identificados, a AWS sugere que os clientes implementem as práticas recomendadas, conforme definido no AWS Well-Architected Tool. Se a melhor prática for implementada, indique que o problema foi resolvido marcando a melhor prática como cumprida no AWS Well-Architected Tool. Se os clientes optarem por não implementar a prática recomendada, a AWS sugere que eles documentem a aprovação do nível de negócios aplicável e os motivos para não implementá-la.

Definir uma workload no AWS Well-Architected Tool

Há duas maneiras de definir uma workload. Na página Workloads no AWS WA Tool, você pode definir uma workload sem um modelo. Ou, na página Modelos de avaliação, você pode usar um modelo de avaliação existente ou criar um modelo para definir uma workload.

Para definir uma workload na página Workloads

1. Selecione Workloads no painel de navegação esquerdo.
2. Selecione o menu suspenso Definir carga de trabalho.
3. Selecione Define workload (Definir carga de trabalho). Ou, se você criou um modelo de avaliação e deseja definir uma workload a partir dele, escolha Definir a partir do modelo de avaliação.
4. Siga as instruções em the section called “Definir uma workload” para especificar as propriedades da workload ou (opcionalmente) aplicar perfis e lentes.

Para definir uma workload na página Modelos de avaliação

1. Selecione Modelos de avaliação no painel de navegação à esquerda.
2. Selecione o nome de um modelo de avaliação existente ou siga as instruções em the section called “Criar um modelo de avaliação” para criar um novo modelo de avaliação.
3. Escolha Definir workload a partir do modelo.
4. Siga as instruções em the section called “Definir uma workload com base em um modelo” para criar a workload a partir do seu modelo de avaliação.

Visualizar uma workload no AWS Well-Architected Tool

Você pode visualizar os detalhes das cargas de trabalho pertencentes a você e daquelas que foram compartilhadas com você.

Para visualizar uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione a carga de trabalho a ser visualizada de uma das seguintes maneiras:
   - Selecione o nome da workload.
   - Selecione a workload e a opção Visualizar detalhes.

A página de detalhes da carga de trabalho será exibida.

> **Note**
>
> Um campo obrigatório, Review owner (Proprietário da revisão), foi adicionado para permitir que você identifique facilmente a pessoa ou o grupo principal responsável pelo processo de revisão.
> Na primeira vez que visualizar uma carga de trabalho que foi definida antes desse campo ser adicionado, você será notificado sobre essa alteração. Selecione Edit (Editar) para definir o campo Review owner (Proprietário da revisão) e nenhuma ação adicional é necessária. Selecione Acknowledge (Confirmar) para adiar a definição do campo Review owner (Proprietário da revisão). Nos próximos 60 dias, um banner será exibido para lembrar você de que o campo está em branco. Para remover o banner, edite a carga de trabalho e especifique um Review owner (Proprietário da revisão).
> Se você não definir o campo até data especificada, o acesso à carga de trabalho será restrito. É possível continuar a visualizar a carga de trabalho e excluí-la, mas você não poderá editá-la, exceto para definir o campo Review owner (Proprietário da revisão). O acesso compartilhado à carga de trabalho não é afetado enquanto o acesso está limitado.

Editar uma workload no AWS Well-Architected Tool

Você pode editar os detalhes de uma carga de trabalho que pertence a você.

Para editar uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione a carga de trabalho que deseja editar e escolha Edit (Editar).
4. Faça as alterações na carga de trabalho.

   Para obter uma descrição de cada um dos campos, consulte Definir uma workload no AWS WA Tool.

   > **Note**
   >
   > Ao atualizar uma workload existente, você pode Ativar o Trusted Advisor, o que cria automaticamente o perfil do IAM para o proprietário da workload. Os proprietários de contas associadas para workloads com a Trusted Advisor ativado precisam criar uma função no IAM. Para obter detalhes, consulte the section called “Ativando Trusted Advisor no IAM”.

5. Selecione Save (Salvar) para salvar as alterações na carga de trabalho.

   Se um campo obrigatório ficar em branco, ou se um valor especificado não for válido, será necessário corrigir o problema antes que as atualizações na carga de trabalho sejam salvas.

Compartilhar uma workload no AWS Well-Architected Tool

Você pode compartilhar uma workload que você possui com outras Contas da AWS, usuários, uma organização e unidades organizacionais (OUs) na mesma Região da AWS.

> **Note**
>
> Você só pode compartilhar workloads na mesma Região da AWS.
> Ao compartilhar uma workload com outra Conta da AWS, se o destinatário não tiver a permissão `wellarchitected:UpdateShareInvitation`, ele não poderá aceitar o convite de compartilhamento. Consulte the section called “Conceder acesso ao AWS WA Tool” para ver exemplos de políticas de permissão.

Para compartilhar uma workload com outras Contas da AWS e usuários

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione uma workload que possui usando uma das seguintes formas:
   - Selecione o nome da workload.
   - Selecione a workload e a opção Visualizar detalhes.
4. Escolha Compartilhamentos. Depois, escolha Criar e Criar compartilhamentos para usuários ou contas para criar um convite de workload.
5. Insira o ID de 12 dígitos da Conta da AWS ou o ARN do usuário com o qual deseja compartilhar a workload.
6. Escolha a permissão que deseja conceder.

   Somente leitura

   Fornece acesso somente leitura à workload.

   Colaborador

   Fornece acesso de atualização a respostas e observações, e acesso somente leitura ao restante da workload.
7. Escolha Criar para enviar um convite de workload para a Conta da AWS ou o usuário especificado.

Se o convite de carga de trabalho não for aceito em até sete dias, ele expirará automaticamente.

Se um usuário e a Conta da AWS do usuário tiverem convites de workload, o convite de workload com a permissão de nível mais alto será aplicado ao usuário.

> **Important**
>
> Antes de compartilhar uma workload com uma organização ou unidades organizacionais (UOs), você deve habilitar o acesso do AWS Organizations.

Para compartilhar uma workload com sua organização ou UOs

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione uma workload que possui usando uma das seguintes formas:
   - Selecione o nome da workload.
   - Selecione a workload e a opção Visualizar detalhes.
4. Escolha Compartilhamentos. Depois, escolha Criar e Criar compartilhamentos para organizações.
5. Na página Criar compartilhamento de workload, escolha se deseja conceder permissões a toda a organização ou a uma ou mais UOs.
6. Escolha a permissão que deseja conceder.

   Somente leitura

   Fornece acesso somente leitura à workload.

   Colaborador

   Fornece acesso de atualização a respostas e observações, e acesso somente leitura ao restante da workload.
7. Escolha Criar para compartilhar a workload.

Para ver quem compartilhou acesso a uma carga de trabalho, escolha Shares (Compartilhamentos) na página Visualizar detalhes da workload no AWS Well-Architected Tool.

Para impedir que uma entidade compartilhe cargas de trabalho, anexe uma política que negue ações `wellarchitected:CreateWorkloadShare`.

Também é possível compartilhar lentes personalizadas que você possui com outros usuários de Contas da AWS, sua organização e UOs na mesma Região da AWS. Para obter detalhes, consulte Compartilhar uma lente personalizada no AWS WA Tool.

Considerações ao compartilhar workloads do AWS Well-Architected Tool

Uma workload pode ser compartilhada com até 20 Contas da AWS e usuários diferentes. Uma workload só pode ser compartilhada com contas e usuários que estejam na mesma Região da AWS dela.

Para compartilhar uma workload em uma região introduzida após 20 de março de 2019, tanto você como a Conta da AWS compartilhada devem habilitar a região no AWS Management Console. Para obter mais informações, consulte Infraestrutura global da AWS.

Você pode compartilhar uma workload com uma Conta da AWS, com usuários individuais em uma conta ou com ambos. Quando você compartilha uma workload com uma Conta da AWS, todos os usuários dessa conta recebem acesso à workload. Se apenas usuários específicos de uma conta precisarem de acesso, siga a prática recomendada de conceder privilégio mínimo e compartilhe a workload individualmente com esses usuários.

Se tanto uma Conta da AWS quanto um usuário na conta tiverem convites de workload, o convite de workload com as permissões de nível mais alto determinará a permissão do usuário para a workload. Se você excluir o convite de workload para o usuário, o acesso dele será determinado pelo convite de workload para a Conta da AWS. Exclua ambos os convites de carga de trabalho para remover o acesso do usuário à carga de trabalho.

Antes de compartilhar uma workload com uma organização ou uma ou mais unidades organizacionais (UOs), você deve habilitar o acesso do AWS Organizations.

Se você compartilha uma workload com uma organização e com uma ou mais OUs, o convite de workload com as permissões de nível mais alto determina a permissão da conta para a workload.

Para habilitar o compartilhamento do AWS Organizations

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Configurações.
3. Escolha Habilitar suporte do AWS Organizations.
4. Escolha Salvar configurações.

Excluir acesso compartilhado no AWS Well-Architected Tool

Você pode excluir um convite de carga de trabalho. Excluir um convite de carga de trabalho removerá o acesso compartilhado à carga de trabalho.

Como excluir um acesso compartilhado a uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione a carga de trabalho usando uma das seguintes formas:
   - Selecione o nome da workload.
   - Selecione a workload e a opção Visualizar detalhes.
4. Escolha Compartilhamentos.
5. Selecione o convite de carga de trabalho a ser excluído e escolha Delete (Excluir).
6. Escolha Delete para confirmar.

Se um usuário e a Conta da AWS do usuário tiverem convites de workload, será necessário excluir os dois convites de workload para remover a permissão do usuário para a workload.

Modificar o acesso compartilhado no AWS Well-Architected Tool

Você pode modificar um convite de carga de trabalho pendente ou aceito.

Como modificar o acesso compartilhado a uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione uma workload que possui usando uma das seguintes formas:
   - Selecione o nome da workload.
   - Selecione a workload e a opção Visualizar detalhes.
4. Escolha Compartilhamentos.
5. Selecione o convite de carga de trabalho a ser modificado e escolha Edit (Editar).
6. Escolha a nova permissão que deseja conceder ao usuário ou à Conta da AWS.

Somente leitura

Fornece acesso somente leitura à workload.

Colaborador

Fornece acesso de atualização a respostas e observações, e acesso somente leitura ao restante da workload.

7. Escolha Salvar.

Se o convite de carga de trabalho modificado não for aceito em até sete dias, ele expirará automaticamente.

Aceitar e rejeitar convites de workload no AWS Well-Architected Tool

Um convite de workload é uma solicitação para compartilhar uma workload que pertence a outra Conta da AWS. Se você aceitar o convite de carga de trabalho, a carga de trabalho será incluída nas páginas Workloads (Cargas de trabalho) e Dashboard (Painel). Se você rejeitar o convite de carga de trabalho, ele será removido da lista de convites de carga de trabalho.

Você tem sete dias para aceitar um convite de carga de trabalho. Se você não aceitar o convite em até sete dias, ele expirará automaticamente.

> **Note**
>
> As workloads só podem ser compartilhadas na mesma Região da AWS.

Como aceitar ou rejeitar um convite de carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Workload invitations (Convites de carga de trabalho).
3. Selecione o convite de carga de trabalho a ser aceito ou rejeitado.
   - Para aceitar o convite de carga de trabalho, escolha Accept (Aceitar).

A carga de trabalho será adicionada às páginas Workloads (Cargas de trabalho) e Dashboard (Painel).

- Para rejeitar o convite de carga de trabalho, escolha Reject (Rejeitar).

  O convite de carga de trabalho será removido da lista.

Para rejeitar o acesso compartilhado após um convite de carga de trabalho ter sido aceito, escolha Reject share (Rejeitar compartilhamento) na página Visualizar detalhes da workload no AWS Well-Architected Tool da carga de trabalho.

Excluir uma workload no AWS Well-Architected Tool

Você pode excluir uma carga de trabalho quando ela não for mais necessária. A exclusão de uma carga de trabalho removerá todos os dados associados a ela, incluindo todos os marcos e os convites de compartilhamento de carga de trabalho. Somente o proprietário de uma workload poderá excluí-la.

> **Warning**
>
> A exclusão de uma workload não pode ser desfeita. Todos os dados associados à carga de trabalho serão removidos permanentemente.

Para excluir uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione a carga de trabalho que deseja excluir e selecione Delete (Excluir).
4. Na janela Delete (Excluir), selecione Delete (Excluir) para confirmar a exclusão da carga de trabalho e de seus marcos.

Para impedir que uma entidade exclua cargas de trabalho, anexe uma política que negue ações `wellarchitected:DeleteWorkload`.

Gerar um relatório de workload no AWS Well-Architected Tool

Você pode gerar um relatório da carga de trabalho para uma perspectiva. O relatório contém as respostas às perguntas sobre a carga de trabalho, suas notas e o número atual de riscos altos e médios identificados. Se uma pergunta tem um ou mais riscos identificados, o plano de melhoria associado a essa pergunta lista as ações a serem executadas para reduzir esses riscos.

Se a workload tiver um perfil associado, as informações gerais do perfil e os riscos priorizados serão exibidos no relatório da workload.

Um relatório permite que você compartilhe detalhes sobre a carga de trabalho com outras pessoas que não tenham acesso ao AWS Well-Architected Tool.

Como gerar um relatório da carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione a workload desejada e escolha Visualizar detalhes.
4. Selecione a perspectiva para a qual deseja gerar um relatório e escolha Generate report (Gerar relatório).

   O relatório será gerado e você poderá fazer download dele ou visualizá-lo.

Visualizar detalhes da workload no AWS Well-Architected Tool

A página de detalhes da carga de trabalho oferece informações sobre a carga de trabalho, incluindo os marcos, o plano de melhoria e todos os compartilhamentos de carga de trabalho. Use as guias na parte superior da página para navegar até diferentes seções de detalhes.

Para excluir a carga de trabalho, escolha Delete workload (Excluir carga de trabalho). Somente o proprietário de uma workload poderá excluí-la.

Para remover o acesso a uma carga de trabalho compartilhada, escolha Reject share (Rejeitar compartilhamento).

Tópicos

- Guia Visão geral do AWS Well-Architected Tool

- Guia Etapas do AWS Well-Architected Tool
- Guia Propriedades do AWS Well-Architected Tool
- Guia Compartilhamentos do AWS Well-Architected Tool

Guia Visão geral do AWS Well-Architected Tool

Inicialmente, quando você visualiza uma carga de trabalho, a guia Overview (Visão geral) é a primeira informação exibida. Essa guia fornece o estado geral da carga de trabalho seguido pelo estado de cada perspectiva.

Se você não tiver concluído todas as perguntas, será exibido um banner para lembrá-lo de iniciar ou continuar a documentar sua carga de trabalho.

A seção Workload overview (Visão geral da carga de trabalho) mostra o estado geral atual da carga de trabalho e quaisquer Workload notes (Notas da carga de trabalho) que você tenha inserido. Selecione Edit (Editar) para atualizar o estado ou as notas.

Para capturar o estado atual da carga de trabalho, selecione Save milestone (Salvar marco). Os marcos são imutáveis e não poderão ser alterados depois de serem salvos.

Para continuar documentando o estado da carga de trabalho, escolha Start reviewing (Iniciar a revisão) e selecione a perspectiva desejada.

Guia Etapas do AWS Well-Architected Tool

Para exibir os marcos da carga de trabalho, selecione a guia Milestones (Marcos).

Depois de selecionar um marco, selecione Generate report (Gerar relatório) para criar o relatório da carga de trabalho associada a esse marco. O relatório contém as respostas às perguntas sobre a carga de trabalho, suas notas e o número de riscos altos e médios na carga de trabalho no momento em que o marco foi salvo.

Você pode visualizar detalhes sobre o estado da carga de trabalho no momento de um marco específico com uma destas opções:

- Selecionando o nome do marco.
- Selecionando o marco e a opção View milestone (Visualizar marco).

Guia Propriedades do AWS Well-Architected Tool

Para exibir as propriedades da carga de trabalho, selecione a guia Properties (Propriedades). Inicialmente, essas propriedades são os valores que foram especificados quando a carga de trabalho foi definida. Escolha Edit (Editar) para fazer alterações. Somente o proprietário da carga de trabalho pode fazer alterações.

Para obter descrições das propriedades, consulte Definir uma workload no AWS WA Tool.

Guia Compartilhamentos do AWS Well-Architected Tool

Para exibir ou modificar os convites de carga de trabalho, escolha a guia Shares (Compartilhamentos). Esta guia é exibida somente para o proprietário de uma carga de trabalho.

As informações a seguir são exibidas para cada usuário e Conta da AWS que tem acesso compartilhado à workload:

Entidade principal

O ID da Conta da AWS ou o ARN do usuário com acesso compartilhado à workload.

Status

O status do convite da carga de trabalho.

- Pendente

  O convite está aguardando para ser aceito ou rejeitado. Se um convite de carga de trabalho não for aceito em até sete dias, ele expirará automaticamente.

- Aceito

  O convite foi aceito.

- Rejeitado

  O convite foi rejeitado.

- Expirada

  O convite não foi aceito nem rejeitado no prazo de sete dias.

Permissão

A permissão concedida ao usuário ou à Conta da AWS.

- Somente leitura

  O principal tem acesso somente leitura à carga de trabalho.

- Colaborador

  O principal pode atualizar respostas e observações e tem acesso somente leitura ao restante da carga de trabalho.

Detalhes de permissões

Descrição detalhada da permissão

Para compartilhar a workload com outra conta ou usuário da Conta da AWS na mesma Região da AWS, selecione Criar. Uma workload pode ser compartilhada com até 20 Contas da AWS e usuários diferentes.

Para excluir um convite de carga de trabalho, selecione o convite e escolha Delete (Excluir).

Para modificar um convite de carga de trabalho, selecione o convite e escolha Edit (Editar).

Usar lentes no AWS WA Tool

No AWS Well-Architected Tool, você pode usar lentes para avaliar de forma consistente suas arquiteturas em relação às práticas recomendadas e identificar áreas que precisam de melhoria. As lentes do AWS Well-Architected Framework são aplicados automaticamente quando uma workload é definida.

Uma carga de trabalho pode ter uma ou mais perspectivas aplicadas. Cada perspectiva tem seu próprio conjunto de perguntas, melhores práticas, notas e plano de melhoria.

Dois tipos de lente podem ser aplicados às workloads: lentes do Catálogo de lentes e Lentes personalizadas.

- Catálogo de lentes: lentes oficiais criadas e mantidas pela AWS. O Catálogo de lentes está disponível para todos os usuários e não requer nenhuma instalação adicional para ser usado.
- Lentes personalizadas: lentes definidas pelo usuário que não são conteúdo oficial da AWS. Você pode criar lentes personalizadas com seus próprios pilares, perguntas, práticas recomendadas e plano de aprimoramento, assim como compartilhar lentes personalizadas com outras Contas da AWS.

Cinco lentes podem ser adicionadas por vez a uma workload e no máximo 20 lentes podem ser aplicadas a uma workload.

Se uma perspectiva for removida de uma carga de trabalho, os dados associados à perspectiva serão retidos. Os dados serão restaurados se você adicionar a perspectiva novamente à carga de trabalho.

Adicionar uma lente a uma workload no AWS WA Tool

Ao adicionar uma lente a uma workload, você consegue entender melhor os pontos fortes e fracos de sua arquitetura, identificar melhorias e garantir que as workloads sigam as práticas recomendadas.

Para adicionar uma perspectiva a uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.

3. Selecione a workload desejada e escolha Visualizar detalhes.
4. Selecione a lente a ser adicionada e escolha Salvar.

   As lentes podem ser selecionadas em Lentes personalizadas, Catálogo de lentes ou ambas.

Até 20 lentes podem ser adicionadas a uma workload.

Para obter mais informações sobre o Catálogo de lentes da AWS, acesse AWS Well-Architected Lenses. Nem todo white paper sobre lentes é fornecido como lente no Catálogo de lentes.

> **Isenção de responsabilidade**
>
> Ao acessar e/ou aplicar lentes personalizadas criadas por outro usuário ou conta da AWS, você reconhece que as lentes personalizadas criadas por outros usuários e compartilhadas com você são Conteúdo de Terceiros, conforme definido no Contrato do Cliente da AWS.

Remover uma lente de uma workload no AWS WA Tool

Se uma lente não for mais relevante para sua workload, você poderá removê-la.

Para remover uma perspectiva de uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, selecione Workloads.
3. Selecione a workload desejada e escolha Visualizar detalhes.
4. Desmarque a lente a ser removida e escolha Salvar.

   As lentes do AWS Well-Architected Framework não podem ser removidas de uma workload.

Os dados associados à perspectiva são mantidos. Se a lente for adicionada novamente à carga de trabalho, os dados serão restaurados.

Visualizar detalhes da lente para uma workload no AWS WA Tool

Você pode visualizar detalhes sobre as lentes no console do AWS Well-Architected Tool. Para visualizar detalhes sobre uma perspectiva, selecione-a.

Guia Visão geral

A guia Overview (Visão geral) fornece informações gerais sobre a perspectiva, como o número de perguntas respondidas. Nessa guia, você pode continuar revisando uma carga de trabalho, gerar um relatório ou editar as notas da perspectiva.

Guia Plano de melhoria

A guia Improvement plan (Plano de melhoria) fornece uma lista de ações recomendadas para melhorar a carga de trabalho. É possível filtrar as recomendações com base no risco e no pilar.

Guia Compartilhamentos

Para uma lente personalizada, a guia Compartilhamentos fornece uma lista de entidades principais do IAM com as quais a lente foi compartilhada.

Lentes personalizadas para workloads no AWS WA Tool

Você pode criar lentes personalizadas com seus próprios pilares, perguntas, práticas recomendadas e plano de aprimoramento. Você aplica lentes personalizadas a uma workload da mesma forma que aplica as lentes fornecidas pela AWS. Você também pode compartilhar as lentes personalizadas que criar com outras Contas da AWS, e as lentes personalizadas de propriedade de outras pessoas podem ser compartilhadas com você.

Você pode adaptar as perguntas em uma lente personalizada para serem específicas a uma tecnologia específica, ajudá-lo a atender às necessidades de governança em sua organização ou ampliar a orientação fornecida pelo Well-Architected Framework e pelas lentes da AWS. Assim como as lentes existentes, você pode acompanhar o progresso ao longo do tempo criando marcos e fornecer status periódico gerando relatórios.

Tópicos

- Visualizar lentes personalizadas no AWS WA Tool
- Criar uma lente personalizada para uma workload no AWS WA Tool
- Visualizar uma lente personalizada para uma workload no AWS WA Tool
- Publicar uma lente personalizada no AWS WA Tool pela primeira vez
- Publicar uma atualização em uma lente personalizada no AWS WA Tool
- Compartilhar uma lente personalizada no AWS WA Tool

- Adicionar tags a uma lente personalizada no AWS WA Tool
- Excluir uma lente personalizada no AWS WA Tool
- Especificação do formato da lente no AWS WA Tool

Visualizar lentes personalizadas no AWS WA Tool

Você pode visualizar os detalhes das lentes personalizadas que possui e das lentes personalizadas que foram compartilhadas com você.

Para visualizar uma lente

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.

   > **Note**
   >
   > A seção Lentes personalizadas estará vazia se você não tiver criado uma lente personalizada ou tiver uma lente personalizada compartilhada com você.

3. Escolha quais lentes personalizadas você deseja visualizar:
   - De minha propriedade: mostra lentes personalizadas que você criou.
   - Compartilhado comigo: mostra lentes personalizadas que foram compartilhadas com você.
4. Selecione a lente personalizada para visualizar em uma das seguintes formas:
   - Escolha o nome da lente.
   - Selecione a lente e escolha Exibir detalhes.

A página Visualizar detalhes da lente para uma workload no AWS WA Tool será exibida.

A página Lentes personalizadas tem os seguintes campos:

Name

O nome da lente.

Proprietário

O ID da Conta da AWS que possui a lente personalizada.

Status

Um status de PUBLISHED significa que a lente personalizada foi publicada e pode ser aplicada a workloads ou compartilhada com outras Contas da AWS.

Um status de DRAFT significa que a lente personalizada foi criada, mas ainda não foi publicada. Uma lente personalizada deve ser publicada antes de ser aplicada às workloads ou compartilhada.

Versão

O nome da versão da lente personalizada.

Última atualização

Data e hora em que as lentes personalizadas foram atualizadas pela última vez.

Criar uma lente personalizada para uma workload no AWS WA Tool

Para criar uma lente personalizada

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.
3. Escolha Criar ação personalizada.
4. Escolha Baixar arquivo para baixar o arquivo de modelo JSON.
5. Abra o arquivo de modelo JSON com seu editor de texto favorito e adicione os dados de sua lente personalizada. Esses dados incluem seus pilares, perguntas, práticas recomendadas e links de planos de aprimoramento.

   Para mais detalhes, consulte Especificação do formato da lente no AWS WA Tool. Uma lente personalizada não pode exceder 500 KB de tamanho.
6. Escolha Escolher arquivo para selecionar seu arquivo JSON.
7. (Opcional) Na seção Tags, adicione as tags que você deseja associar à workload.
8. Escolha Enviar e visualizar para visualizar a lente personalizada ou Enviar para enviar a lente personalizada sem pré-visualizar.

Se você optar por Enviar e visualizar sua lente personalizada, poderá selecionar Próximo para navegar pela visualização prévia da lente ou selecionar Sair da visualização para voltar às Lentes personalizadas.

Se a validação falhar, edite seu arquivo JSON e tente criar a lente personalizada novamente.

Depois que o AWS WA Tool validar seu arquivo JSON, sua lente personalizada será exibida em Lentes personalizadas.

Depois que uma lente personalizada é criada, ela fica no status DRAFT. Você deve publicar a lente antes que ela possa ser aplicada a workloads ou compartilhada com outras Contas da AWS.

Você pode criar até 15 lentes personalizadas em uma Conta da AWS.

> **Isenção de responsabilidade**
>
> Não inclua nem colete informações de identificação pessoal (PII) de usuários finais ou de outros indivíduos identificáveis em suas lentes personalizadas ou por meio delas. Se suas lentes personalizadas ou aquelas compartilhadas com você e usadas em sua conta incluírem ou coletarem PII, você será responsável por: garantir que essa informações incluídas sejam processadas de acordo com a legislação aplicável, fornecer avisos de privacidade adequados e obter os consentimentos necessários para o processamento desses dados.

Visualizar uma lente personalizada para uma workload no AWS WA Tool

Para visualizar uma lente personalizada

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.
3. Somente lentes com status DRAFT podem ser visualizadas. Selecione a lente personalizada DRAFT desejada e escolha a Experiência de visualização.
4. Escolha Próximo para navegar pela visualização prévia da lente.
5. (Opcional) Você pode revisar seu Plano de melhoria selecionando as melhores práticas em cada pergunta na pré-visualização e escolhendo Atualizar com base nas respostas para testar sua

lógica de risco. Se houver necessidade de alterações, você pode atualizar as Regras de risco em seu modelo JSON antes de publicar.

6. Escolha Sair da visualização para voltar à lente personalizada.

> **Note**
>
> Você também pode visualizar uma lente personalizada selecionando Enviar e visualizar ao Criar uma lente personalizada.

Publicar uma lente personalizada no AWS WA Tool pela primeira vez

Para publicar uma lente personalizada

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.
3. Selecione a lente personalizada desejada e escolha Publicar lente.
4. Na caixa Nome da versão, insira um identificador exclusivo para a alteração da versão. Esse valor pode ter até 32 caracteres e deve conter somente caracteres alfanuméricos e pontos (“.”).
5. Escolha Publicar lentes personalizadas.

   Depois que uma lente personalizada é publicada, ela fica com o status PUBLISHED.

A lente personalizada agora pode ser aplicada a workloads ou compartilhada com outros usuários ou Contas da AWS.

Publicar uma atualização em uma lente personalizada no AWS WA Tool

Para publicar uma atualização em uma lente personalizada existente

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.
3. Selecione a lente personalizada desejada e escolha Editar.

4. Se você não tiver um arquivo JSON atualizado pronto, escolha Baixar arquivo para baixar uma cópia da lente personalizada atual. Edite o arquivo JSON baixado com seu editor de texto favorito e faça as alterações desejadas.
5. Escolha Escolher arquivo para selecionar seu arquivo JSON atualizado e escolha Enviar e visualizar para visualizar a lente personalizada ou Enviar para enviar a lente personalizada sem visualizar.

   Uma lente personalizada não pode exceder 500 KB de tamanho.

   Depois que AWS WA Tool validar seu arquivo JSON, sua lente personalizada será exibida em Lentes personalizadas no status RASCUNHO.
6. Selecione a lente personalizada desejada e escolha Publicar lente.
7. Escolha Revisar alterações antes de publicar para verificar se as alterações feitas em sua lente personalizada estão corretas. Isso inclui a validação de:

   - O nome da lente personalizada
   - Os nomes dos pilares
   - As perguntas novas, atualizadas e excluídas

   Escolha Próximo.
8. Especifique o tipo de alteração de versão.

   Versão principal

   Indica que mudanças substanciais foram feitas na lente. Use para alterações que afetam o significado da lente personalizada.

   Qualquer workload com a lente aplicada será notificada de que uma nova versão da lente personalizada está disponível.

   As principais alterações de versão não são aplicadas automaticamente às workloads usando a lente.

   Versão secundária

   Indica que foram feitas pequenas alterações na lente. Use para pequenas alterações, como alterações de texto ou atualizações nos links de URL.

Pequenas alterações de versão são aplicadas automaticamente às workloads que usam a lente personalizada.

Escolha Próximo.

9. Na caixa Nome da versão, insira um identificador exclusivo para a alteração da versão. Esse valor pode ter até 32 caracteres e deve conter somente caracteres alfanuméricos e pontos (“.”).
10. Escolha Publicar lentes personalizadas.

    Depois que uma lente personalizada é publicada, ela fica com o status PUBLISHED.

A lente personalizada atualizada agora pode ser aplicada a workloads ou compartilhada com outros usuários ou Contas da AWS.

Se a atualização for uma alteração importante na versão, todas as workloads com a versão anterior da lente aplicada serão notificadas de que uma nova versão está disponível e terão a opção de atualização.

As atualizações de versões menores são aplicadas automaticamente sem qualquer notificação.

Você pode criar até 100 versões de lentes personalizadas.

Compartilhar uma lente personalizada no AWS WA Tool

Você pode compartilhar uma lente personalizada com outras Contas da AWS, usuários, AWS Organizations e unidades organizacionais (OUs).

Para compartilhar uma lente personalizada com outras pessoas Contas da AWS e usuários

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.
3. Selecione a lente personalizada a ser compartilhada e escolha Exibir detalhes.
4. Na página Visualizar detalhes da lente para uma workload no AWS WA Tool, selecione Compartilhamentos. Em seguida, escolha Criar e Criar compartilhamentos com usuários ou contas para criar um convite de compartilhamento de lentes.
5. Digite o ID da Conta da AWS de 12 dígitos ou o ARN do usuário com o qual você deseja compartilhar a lente personalizada.

6. Escolha Criar para enviar um convite de compartilhamento de lente para a Conta da AWS ou o usuário especificado.

Você pode compartilhar lentes personalizadas com até 300 usuários ou Contas da AWS.

Se o convite para o compartilhamento de lentes não for aceito dentro de sete dias, o convite expirará automaticamente.

> **Important**
>
> Antes de compartilhar uma lente personalizada com uma organização ou unidades organizacionais (OUs), você deve habilitar o acesso do AWS Organizations.

Para compartilhar uma lente personalizada com sua organização ou OUs

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.
3. Selecione a lente personalizada a ser compartilhada.
4. Na página Visualizar detalhes da lente para uma workload no AWS WA Tool, selecione Compartilhamentos. Depois, escolha Criar e Criar compartilhamentos para organizações.
5. Na página Criar compartilhamento de lente personalizado, escolha se deseja conceder permissões a toda a organização ou a uma ou mais OUs.
6. Escolha Criar para compartilhar a lente personalizada.

Para ver quem tem acesso compartilhado a uma lente personalizada, selecione Compartilhamentos na página Visualizar detalhes da lente para uma workload no AWS WA Tool.

> **Isenção de responsabilidade**
>
> Ao compartilhar suas lentes personalizadas com outras Contas da AWS, você reconhece que a AWS disponibilizará suas lentes personalizadas para essas outras contas. Essas outras contas podem continuar acessando e usando suas lentes personalizadas compartilhadas, mesmo que você as exclua de sua própria Conta da AWS ou encerre sua Conta da AWS.

Adicionar tags a uma lente personalizada no AWS WA Tool

Para adicionar tags a uma lente personalizada

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.
3. Selecione a lente personalizada que deseja atualizar.
4. Na seção Tags, escolha Gerenciar tags.
5. Selecione Adicionar nova tag e digite a Chave e o Valor de cada tag que deseja adicionar.
6. Selecione Salvar.

Para remover uma tag, selecione Remover ao lado da tag que você deseja remover.

Excluir uma lente personalizada no AWS WA Tool

Para excluir uma lente personalizada

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. No painel de navegação à esquerda, escolha Lentes personalizadas.
3. Selecione a lente personalizada a ser excluída e escolha Excluir.
4. Escolha Excluir.

   As workloads existentes com a lente aplicada são notificadas de que a lente personalizada foi excluída, mas podem continuar a usá-la. A lente personalizada não pode mais ser aplicada a novas workloads.

> **Isenção de responsabilidade**
>
> Ao compartilhar suas lentes personalizadas com outras Contas da AWS, você reconhece que a AWS disponibilizará suas lentes personalizadas para essas outras contas. Essas outras contas podem continuar acessando e usando suas lentes personalizadas compartilhadas, mesmo que você as exclua de sua própria Conta da AWS ou encerre sua Conta da AWS.

Especificação do formato da lente no AWS WA Tool

As lentes são definidas usando um formato JSON específico. Ao começar a criar uma lente personalizada, você tem a opção de baixar um arquivo JSON de modelo. Você pode usar esse arquivo como base para suas lentes personalizadas, pois ele define a estrutura básica dos pilares, das perguntas, das melhores práticas e do plano de melhoria.

Seção de lentes

Esta seção define os atributos da própria lente personalizada. Este é o nome e a descrição.

- `schemaVersion`: A versão do esquema de lente personalizada a ser usada. Definido pelo modelo, não altere.
- `name`: Nome da lente. O nome pode ter até 128 caracteres.
- `description`: Descrição em texto da lente. Esse texto é exibido ao selecionar lentes para adicionar durante a criação da workload ou ao selecionar uma lente para aplicar a uma workload existente posteriormente. A descrição pode ter até 2.048 caracteres.

```
   "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.",
```

Seção de pilares

Esta seção define os pilares associados à lente personalizada. Você pode mapear suas perguntas para os pilares do AWS Well-Architected Framework, definir seus próprios pilares ou ambos.

Você pode definir até dez pilares em uma lente personalizada.

- `id`: ID do pilar. O ID pode ter entre 3 e 128 caracteres e conter somente caracteres alfanuméricos e sublinhado (“_”). Os IDs usados em um pilar devem ser exclusivos.

  Ao mapear suas perguntas para os pilares da Estrutura, use os seguintes IDs:

  - `operationalExcellence`
  - `security`

  - `reliability`
  - `performance`
  - `costOptimization`
  - `sustainability`
- `name`: Nome do pilar. O nome pode ter até 128 caracteres.

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

Seção de perguntas

Esta seção define as questões associadas a um pilar.

Você pode definir até 20 perguntas em um pilar em uma lente personalizada.

- `id`: ID da pergunta. A ID pode ter de 3 a 128 caracteres e conter apenas caracteres alfanuméricos e de sublinhado ("_"). As IDs usadas em uma pergunta devem ser exclusivas.
- `title`: Título da pergunta. O título pode ter até 128 caracteres.
- `description`: Descreve a pergunta com mais detalhes. A descrição pode ter até 2.048 caracteres.
- `helpfulResource displayText`: opcional. Texto que fornece informações úteis sobre a pergunta. O texto pode ter até 2.048 caracteres. Deve ser especificado se `helpfulResource url` for especificado.

- `helpfulResource url`: opcional. Um recurso de URL que explica a pergunta com mais detalhes. O URL deve começar com `http://` ou `https://`.

> **Note**
>
> Ao sincronizar uma workload da lente personalizada com o Jira, as perguntas exibem o “ID” e o “título” da pergunta.
> O formato usado nos tíquetes do Jira é `[ QuestionID ] QuestionTitle`.

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

Seção de opções

Esta seção define as opções associadas a uma pergunta.

Você pode definir até 15 opções para uma pergunta em uma lente personalizada.

- `id`: ID da escolha. O ID pode ter entre 3 e 128 caracteres e conter somente caracteres alfanuméricos e sublinhado (“_”). Um ID exclusivo deve ser especificado para cada opção em uma pergunta. A adição de uma opção com um sufixo _no funcionará como uma opção `None of these` para a pergunta.
- `title`: Título da escolha. O título pode ter até 128 caracteres.
- `helpfulResource displayText`: opcional. Texto que fornece informações úteis sobre uma opção. O texto pode ter até 2.048 caracteres. Deverá ser incluído se `helpfulResource url` for especificado.
- `helpfulResource url`: opcional. Um recurso de URL que explica a escolha em mais detalhes. O URL deve começar com `http://` ou `https://`.
- `improvementPlan displayText`: Texto que descreve como uma escolha pode ser aprimorada. O texto pode ter até 2.048 caracteres. É necessário um `improvementPlan` para cada opção, exceto para uma opção `None of these`.
- `improvementPlan url`: opcional. Um recurso de URL que pode ajudar na melhoria. O URL deve começar com `http://` ou `https://`.
- `additionalResources type`: opcional. O tipo de recursos adicionais. O valor pode ser `HELPFUL_RESOURCE` ou `IMPROVEMENT_PLAN`.
- `additionalResources content`: opcional. Especifica os valores `displayText` e `url` para o recurso adicional. Até cinco recursos úteis adicionais e até cinco itens adicionais do plano de melhoria podem ser especificados para uma escolha.
  - `displayText`: opcional. Texto que descreve o recurso útil ou o plano de melhoria. O texto pode ter até 2.048 caracteres. Deverá ser incluído se `url` for especificado.
  - `url`: opcional. Um recurso de URL para o recurso útil ou plano de melhoria. O URL deve começar com `http://` ou `https://`.

> **Note**
>
> Ao sincronizar uma workload da lente personalizada com o Jira, as opções exibem o “ID” da pergunta e da escolha, bem como o “título” da escolha.

O formato usado é `[ QuestionID | ChoiceID ] ChoiceTitle`.

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

```
                ]
              },
              {
                "type": "IMPROVEMENT_PLAN",
                "content": [
                  {
                    "displayText": "This is additional text that will be shown for
improvement of this choice.",
                    "url": "https://example.com/popt02_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"
             }

           }
```

Seção de regras de risco

Esta seção define como as opções selecionadas determinam o nível de risco.

Você pode definir no máximo três regras de risco por pergunta, uma para cada nível de risco.

- `condition`: Uma expressão booleana das opções mapeada para um nível de risco para a pergunta, ou `default`.

  Deve haver uma regra de risco `default` para cada pergunta.
- `risk`: Indica o risco associado à condição. Os valores válidos são `HIGH_RISK`, `MEDIUM_RISK` e `NO_RISK`.

A ordem de suas regras de risco é significativa. O primeiro `condition` que é avaliado como `true` define o risco para a pergunta. Um padrão comum para a implementação de regras de risco é começar com as regras menos arriscadas (e, normalmente, mais granulares) e ir descendo até as regras mais arriscadas (e menos específicas).

Por exemplo:

```
"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"
      }
]
```

Se a pergunta tiver três opções (`choice_1`, `choice_2`, e `choice_3`), essas regras de risco resultarão no seguinte comportamento:

- Se todas as três opções forem selecionadas, não há risco.
- Se um `choice_1` ou `choice_2` for selecionado e `choice_3` for selecionado, o risco é médio.
- Se `choice_1` não for selecionado, mas `choice_3` for selecionado, também haverá um risco médio.
- Se nenhuma dessas condições anteriores for verdadeira, o risco é alto.

Atualizações de lente no AWS WA Tool

As lentes do AWS Well-Architected Framework e outras lentes fornecidas pela AWS são atualizados à medida que novos serviços são introduzidos, as práticas recomendadas existentes para sistemas baseados em nuvem são refinadas e novas práticas recomendadas são adicionadas. Quando uma nova versão da perspectiva é disponibilizada, o AWS WA Tool é atualizado para refletir as melhores práticas mais recentes. Qualquer nova workload definida usa a nova versão da lente.

A atualização da lente também ocorre quando uma lente personalizada que você aplicou a uma workload ou a um modelo de avaliação tem uma nova versão principal publicada.

Uma atualização de lente pode consistir em qualquer combinação de:

- Adicionar novas perguntas ou melhores práticas
- Remover perguntas ou práticas antigas que não são mais recomendadas
- Atualizar perguntas ou melhores práticas existentes
- Adição ou remoção de pilares

Suas respostas às perguntas existentes são mantidas.

> **Note**
>
> Não é possível desfazer um upgrade de lente. Depois que uma workload for atualizada para a versão mais recente da lente, você não poderá voltar para a versão anterior da lente.

Determinar qual lente atualizar no AWS WA Tool

Você pode descobrir quais workloads não estão usando a versão mais atual da lente visualizando a página Notificações.

As seguintes informações são exibidas na página Notificações para cada workload:

Recurso

O nome da workload ou do modelo de avaliação.

Tipo de recurso

O tipo de recurso. Isso pode ser um modelo de workload ou modele do avaliação.

Recurso associado

O nome da lente.

Tipo de notificação

O tipo de notificação da atualização.

- Not current (Não atual) – a carga de trabalho está usando uma versão da perspectiva que não é mais a atual. Atualize para a versão atual da perspectiva para obter uma melhor orientação.
- Obsoleta: a workload está usando uma versão da lente que não reflete mais as práticas recomendadas. Atualize para a versão atual da perspectiva.
- Excluída: a workload está usando uma lente que foi excluída pelo proprietário.

Versão em uso

A versão da perspectiva usada atualmente para a carga de trabalho.

Versão atual disponível

A versão da lente está disponível para atualização ou Nenhuma se a lente tiver sido excluída.

Para atualizar a perspectiva associada a uma carga de trabalho, selecione a carga de trabalho e escolha Upgrade lens version (Atualizar a versão da perspectiva).

Atualizar uma lente no AWS WA Tool

As lentes podem ser atualizadas para workloads e modelos de avaliação.

> **Note**
>
> Não é possível desfazer uma atualização de lente. Depois que um modelo de workload ou de avaliação tiver sido atualizado para a versão mais recente da lente, você não poderá voltar à versão anterior.

Atualizando uma lente para uma workload

1. Na página Notificações, selecione uma workload da qual fazer upgrade e escolha Atualizar a versão da lente. As informações sobre o que mudou em cada pilar são exibidas.

> **Note**
>
> Você também pode escolher Exibir atualizações disponíveis na guia Visão geral da workload.

2. Antes de atualizar uma lente para uma workload, é criado um marco para salvar o estado da workload existente para referência futura. Insira um nome para o marco no campo Nome do marco.
3. Selecione a caixa Confirmação ao lado de Eu entendo e aceito essas alterações e escolha Salvar.

Depois que a lente for atualizada, você poderá ver a versão anterior da lente na guia Milestones.

Atualizando uma lente para um modelo de avaliação

1. Para atualizar a lente para um modelo de avaliação, escolha
2. Na página Notificações, selecione um modelo de avaliação para atualizar e escolha Atualizar versão da lente. As informações sobre o que mudou em cada pilar são exibidas.

> **Note**
>
> Você também pode escolher Exibir atualizações disponíveis na guia Visão geral da workload.

3. Selecione a caixa de Confirmação ao lado de Eu entendo e aceito essas alterações e escolha Atualizar e editar respostas do modelo para ajustar as respostas às perguntas de práticas recomendadas para seu modelo de avaliação ou Atualizar para atualizar a lente sem ajustar as respostas do modelo.

Catálogo de Lentes para o AWS WA Tool

O Catálogo de Lentes é um conjunto de lentes oficiais da AWS criado pelo AWS Well-Architected Tool que oferecem tecnologia atualizada e práticas recomendadas focadas no setor. O Catálogo de lentes está disponível para todos os usuários e não requer nenhuma instalação adicional para ser usado.

A tabela a seguir descreve todas as lentes oficiais da AWS atualmente disponíveis no Catálogo de lentes.

Nome do perfil	Descrição
Framework Well-Architected da AWS	Aplicadas por padrão a todas as workloads . Conjunto de práticas recomendadas de arquitetura para criar e operar sistemas confiáveis, seguros, eficientes, econômicos e sustentáveis na nuvem.
Mobilidade conectada	Práticas recomendadas para integrar a tecnologia aos sistemas de transporte e aprimorar a experiência geral de mobilidade.
Criação de contêiner	Fornecem práticas recomendadas sobre o processo de design e criação de contêineres.
Data Analytics	Contêm insights coletados pela AWS de estudos de caso reais e ajuda você a aprender os principais elementos de design das workloads de análise do Well-Architected, além de recomendações para melhorias.
DevOps	Descreve uma abordagem estruturada que organizações de todos os portes podem seguir para cultivar uma cultura de alta velocidad e, focada em segurança e capaz de oferecer um valor comercial considerável por meio de tecnologias modernas e práticas recomenda das de DevOps.
Setor de serviços financeiros	Práticas recomendadas para projetar workloads do setor de serviços financeiros na AWS.
IA generativa	Práticas recomendadas para projetar workloads de IA generativa na AWS.

Nome do perfil	Descrição
Governo	Práticas recomendadas para criar e fornecer serviços governamentais na AWS.
Setor de saúde	Práticas recomendadas e orientações sobre como projetar, implantar e gerenciar workloads do setor de saúde na Nuvem AWS.
IoT	Práticas para gerenciar workloads de Internet das Coisas (IoT) na AWS.
Fusões e aquisições	Práticas recomendadas para integração de workloads e migração para a nuvem durante fusões e aquisições.
Machine Learning	Práticas recomendadas para gerenciar workloads e recursos de machine learning na AWS.
Migração	Práticas recomendadas sobre como migrar para a Nuvem AWS.
SaaS	Destinadas a projetar, implantar e arquitetar workloads de software como serviço (SaaS) na Nuvem AWS.
SAP	Princípios de design e práticas recomendadas para workloads do SAP na Nuvem AWS.
Aplicações sem servidor	Práticas recomendadas para criar workloads sem servidor na AWS. Abrange cenários como microsserviços RESTful, back-ends de aplicativos móveis, processamento de fluxos e aplicações web.

Modelos de avaliação no AWS WA Tool

Você pode criar modelos de avaliação no AWS WA Tool que contenham respostas pré-preenchidas para perguntas de práticas recomendadas do Well-Architected Framework e de lentes personalizadas. Os modelos de avaliação do Well-Architected reduzem a necessidade de preencher manualmente as mesmas respostas para as práticas recomendadas que são comuns em várias workloads ao realizar uma revisão do Well-Architected e ajudam a promover a consistência e a padronização das práticas recomendadas entre equipes e workloads.

Você pode criar um modelo de avaliação para responder a perguntas comuns de práticas recomendadas ou criar notas, que podem ser compartilhadas com outro usuário ou conta do IAM, ou com uma organização ou unidade organizacional na mesma Região da AWS. Você pode definir uma workload com base em um modelo de avaliação, o que ajuda a escalar as práticas recomendadas comuns e reduzir a redundância nas workloads.

Criar um modelo de avaliação no AWS WA Tool

Criar um modelo de avaliação

1. Selecione Modelos de avaliação no painel de navegação à esquerda.
2. Selecione Criar modelo.
3. Na página Especificar detalhes do modelo, forneça um nome e uma descrição para seu modelo de avaliação.
4. (Opcional) Nas seções Notas do modelo e Tags, adicione quaisquer notas ou tags do modelo que você deseja associar ao modelo de avaliação. Todas as notas adicionadas são aplicadas a todas as workloads que usam o modelo de avaliação, enquanto as tags são específicas do modelo de avaliação.

   Para obter mais informações sobre tags, consulte Marcando seus Recursos AWS WA Tool.
5. Escolha Próximo.
6. Na página Aplicar lentes, selecione as lentes que você deseja aplicar ao modelo de avaliação. O número máximo de lentes que podem ser aplicadas é de 20.

   As lentes podem ser selecionadas em Lentes personalizadas, Catálogo de lentes ou ambas.

> **Note**
>
> As lentes que são compartilhadas com você não podem ser aplicadas ao modelo de avaliação.

7. Selecione Criar modelo.

Para começar a responder às perguntas do modelo de avaliação que você acabou de criar

1. Na guia Visão geral do modelo, no alerta de informações para Começar a responder perguntas, selecione a lente no menu suspenso Responder perguntas.

> **Note**
>
> Você também pode ir até a seção Lentes, selecionar a lente e escolher Responder perguntas.

2. Para cada lente que você aplicou ao seu modelo de avaliação, responda às perguntas aplicáveis e escolha Salvar e sair quando terminar.

Depois que seu modelo de avaliação for criado, você poderá definir uma nova workload com base nele.

A guia Visão geral do modelo de avaliação deve refletir o número total de perguntas respondidas na seção Detalhes do modelo e as perguntas respondidas para cada lente na seção Lentes.

Editar um modelo de avaliação no AWS WA Tool

Para editar um modelo de avaliação

1. Selecione Modelos de avaliação no painel de navegação à esquerda.
2. Selecione o nome do modelo de avaliação que você deseja editar.
3. Para atualizar as notas de Nome, Descrição ou Notas do modelo para o Modelo de avaliação, escolha Editar na seção Detalhes do modelo da guia Visão geral.
   a. Faça suas alterações em Nome, Descrição ou Observações do modelo.
   b. Escolha Salvar modelo para atualizar o modelo de avaliação com suas alterações.

4. Para atualizar quais lentes são aplicadas ao modelo de avaliação, na seção Lentes da guia Visão geral, escolha Editar lentes aplicadas.
   a. Marque ou desmarque as caixas de seleção das lentes que você deseja adicionar ou remover.

      As lentes podem ser marcadas ou desmarcadas em Lentes personalizadas, Catálogo de lentes ou ambas.
   b. Selecione Salvar modelo para salvar suas alterações.
5. Para atualizar as respostas às perguntas de melhores práticas sobre a lente, na seção Lentes da guia Visão geral, selecione o nome da lente.
   a. Na seção Visão geral da lente, escolha Responder perguntas.

      > **Note**
      >
      > Opcionalmente, você pode selecionar o nome da lente no menu suspenso Modelos de avaliação no painel de navegação esquerdo para acessar a seção Visão geral da lente.
   b. Marque ou desmarque as caixas de seleção ao lado das respostas de melhores práticas que você deseja alterar.
   c. Selecione Salvar e sair para salvar suas alterações.

Compartilhar um modelo de avaliação no AWS WA Tool

Os modelos de avaliação podem ser compartilhados com usuários ou contas, ou podem ser compartilhados com toda uma organização ou unidade organizacional.

Para compartilhar um modelo de avaliação

1. Selecione Modelos de avaliação no painel de navegação à esquerda.
2. Selecione o nome do modelo de avaliação que deseja compartilhar.
3. Escolha a guia Compartilhamentos.
4. Para compartilhar com um usuário ou conta, escolha Criar e selecione Compartilhar com usuários ou contas do IAM. Na caixa Enviar convites, especifique os IDs do usuário ou da conta e escolha Criar.
5. Para compartilhar com uma organização ou unidade organizacional, escolha Criar e selecione Criar compartilhamentos para organizações. Para compartilhar com uma organização inteira, selecione Conceder permissões a toda a organização. Para compartilhar com uma unidade

organizacional, selecione Conceder permissões a unidades organizacionais individuais, especifique a unidade organizacional na caixa e escolha Criar.

> **Important**
>
> Antes de compartilhar um perfil com uma organização ou unidade organizacional (UOs), você deve habilitar o acesso ao AWS Organizations.

Definir uma workload com base em um modelo no AWS WA Tool

É possível definir uma workload com base em um modelo de avaliação que você criou ou de um modelo de avaliação que foi compartilhado com você. Você não pode definir uma nova workload com base em um modelo de avaliação que foi excluído e, se o modelo de avaliação contiver uma versão desatualizada de uma lente, você deverá atualizar o modelo de avaliação antes de poder definir uma nova workload com base nele. Para obter informações sobre como atualizar um modelo de avaliação, consulte the section called “Fazer upgrade de uma lente”.

> **Note**
>
> Para definir uma workload com base em um modelo de avaliação, você deve ter as permissões do IAM para criar uma workload habilitada:`wellarchitected:CreateWorkload`, bem como as seguintes permissões do modelo de avaliação: `wellarchitected:GetReviewTemplate`, `wellarchitected:GetReviewTemplateAnswer`, `wellarchitected:ListReviewTemplateAnswers` e `wellarchitected:GetReviewTemplateLensReview`. Para ter mais informações sobre permissões do IAM, consulte o Guia do usuário do AWS Identity and Access Management.

Para definir uma workload com base em um modelo de avaliação

1. Selecione Modelos de avaliação no painel de navegação à esquerda.
2. Selecione o nome do modelo de avaliação com base no qual você deseja definir uma workload.
3. Escolha Definir workload a partir do modelo.

> **Note**
>
> Você também pode escolher Definir a partir do modelo de avaliação no menu suspenso Definir carga de trabalho na página Workloads.

4. Na etapa Selecionar modelo de avaliação, selecione o cartão do modelo de avaliação e escolha Próximo.
5. Na etapa Especificar propriedades, preencha os campos obrigatórios para as propriedades da workload e escolha Próximo. Para obter mais detalhes, consulte the section called “Definir uma workload”.
6. (Opcional) Na etapa Aplicar perfil, associe um perfil à workload selecionando um perfil existente, pesquisando o nome do perfil ou escolhendo Criar perfil para criar um perfil. Escolha Próximo.

   Os perfis e modelos de avaliação do Well-Architected podem ser usados em conjunto. As perguntas pré-preenchidas em seu modelo de avaliação permanecem respondidas na workload, e as perguntas são priorizadas com base em seu perfil.
7. (Opcional) Na etapa Aplicar lentes, você pode optar por aplicar lentes adicionais de Lentes personalizadas ou do Catálogo de lentes que ainda não foram aplicadas ao modelo de avaliação.
8. Selecione Define workload (Definir carga de trabalho).

Excluir um modelo de avaliação no AWS WA Tool

Para excluir um modelo de avaliação

1. Selecione Modelos de avaliação no painel de navegação à esquerda.
2. Na seção Modelos de avaliação, escolha o modelo de avaliação que você deseja excluir e, no menu suspenso Ações, selecione Excluir.

> **Note**
>
> Você também pode selecionar o nome do modelo e escolher Excluir na guia Visão geral do modelo de avaliação.

3. Na caixa de diálogo Excluir modelo de avaliação, insira o nome do modelo de avaliação no campo para confirmar a exclusão.

4. Escolha Excluir.

Não é possível criar uma workload com base em um modelo de avaliação excluído. Se você compartilhou um modelo de avaliação excluído com outros usuários, contas ou organizações do IAM, eles não poderão criar workloads com base nele.

Usar perfis no AWS WA Tool

Você pode criar perfis para fornecer seu contexto comercial e identificar metas que gostaria de alcançar ao realizar uma revisão do Well-Architected. O AWS Well-Architected Tool usa as informações coletadas do seu perfil para ajudá-lo a se concentrar em uma lista priorizada de perguntas relevantes para sua empresa durante a análise da workload. Anexar um perfil à sua workload também ajuda a ver quais riscos são priorizados para você abordar com seu plano de melhoria.

Você pode criar um perfil na página Perfis e associá-lo a uma nova workload ou adicionar um perfil a uma workload existente.

Criar um perfil

Como criar um perfil

1. Selecione Perfis no painel de navegação à esquerda.
2. Escolha Create profile (Criar perfil).
3. Na seção Propriedades do perfil, forneça um Nome e uma Descrição para seu perfil.
4. Para refinar as informações priorizadas para sua empresa na análise da workload e no plano de melhoria, selecione as respostas mais relevantes para sua empresa na seção Perguntas do perfil.
5. (Opcional) Na seção Tags, adicione as tags que você deseja associar à workload.

   Para obter mais informações sobre tags, consulte Marcando seus Recursos AWS WA Tool.
6. Escolha Salvar. Uma mensagem de sucesso aparece quando o perfil é criado com sucesso.

Quando um perfil é criado, a visão geral do perfil é exibida. A visão geral mostra os dados associados ao perfil, incluindo nome, descrição, ARN, datas de criação e atualização e as respostas às perguntas do perfil. Na página de visão geral do perfil, você pode editar, excluir ou compartilhar seu perfil.

Editar um perfil no AWS WA Tool

Como editar um perfil

1. Selecione Perfis no painel de navegação esquerdo ou escolha Exibir perfil na seção Perfis da workload.
2. Selecione o nome do perfil que deseja atualizar.
3. Escolha Editar na página Visão geral do perfil.
4. Faça as atualizações necessárias nas perguntas do perfil.
5. Escolha Salvar.

Compartilhar um perfil no AWS WA Tool

Os perfis podem ser compartilhados com usuários ou contas, ou podem ser compartilhados com uma organização ou unidade organizacional inteira.

Para compartilhar um perfil

1. Selecione Perfis no painel de navegação à esquerda.
2. Selecione o nome do perfil que deseja compartilhar.
3. Escolha a guia Compartilhamentos.
4. Para compartilhar com um usuário ou conta, escolha Criar e selecione Criar compartilhamentos para usuários ou contas do IAM. Na caixa Enviar convites, especifique os IDs do usuário ou da conta e escolha Criar.
5. Para compartilhar com uma organização ou unidade organizacional, escolha Criar e selecione Criar compartilhamentos para organizações. Para compartilhar com uma organização inteira, selecione Conceder permissões a toda a organização. Para compartilhar com uma unidade organizacional, selecione Conceder permissões para unidades organizacionais individuais, especifique a unidade organizacional na caixa e escolha Criar.

> **Important**
>
> Antes de compartilhar um perfil com uma organização ou unidade organizacional (UOs), você deve habilitar o acesso ao AWS Organizations.

Adicionar um perfil a uma workload no AWS WA Tool

Você pode adicionar um perfil a uma workload existente ou ao definir uma workload para acelerar o processo de revisão dela. O AWS WA Tool usa as informações coletadas do seu perfil para priorizar perguntas na análise da workload que sejam relevantes para sua empresa.

Para obter mais informações sobre como adicionar um perfil ao definir uma workload, consulte the section called “Definir uma workload”.

Para adicionar um perfil a uma workload existente

1. Selecione Workload no painel de navegação esquerdo e selecione o nome da workload que você deseja associar a um perfil.

   > **Note**
   >
   > Somente um perfil pode ser associado a uma workload.

2. Na seção Perfil, escolha Adicionar perfil.
3. Selecione o perfil que você deseja aplicar à workload na lista de perfis disponíveis ou escolha Criar perfil. Para ter mais informações, consulte the section called “Criar um perfil”.
4. Escolha Salvar.

A Visão geral da workload exibe uma contagem de perguntas priorizadas respondidas e riscos priorizados com base nas informações do perfil associado. Escolha Continuar analisando para abordar as questões priorizadas na análise da workload. Para ter mais informações, consulte the section called “Documentar uma workload”.

A seção Perfil exibe o nome, a descrição, o ARN, a versão e a data da última atualização do perfil associado à workload.

Remover um perfil de uma workload no AWS WA Tool

A remoção de um perfil da workload reverte-a para a versão anterior à qual o perfil foi associado, e as questões e os riscos da revisão da workload não são mais priorizados.

Para remover um perfil de uma workload

1. Na seção Perfis da workload, escolha Remover.

2. Para confirmar a remoção, insira o nome do perfil no campo de entrada de texto.
3. Escolha Remover.

Uma notificação de que o perfil foi removido com sucesso da workload é exibida. A remoção de um perfil reverte a workload para a versão anterior à qual o perfil estava associado, e as perguntas e os riscos da análise da workload não são mais priorizados.

Excluir um perfil do AWS WA Tool

Se você criou um perfil, poderá excluí-lo da lista de perfis disponíveis no AWS WA Tool.

A exclusão de um perfil da página Perfis não remove o perfil de nenhuma workload associada. Você pode continuar usando perfis que foram compartilhados e associados a uma workload antes da exclusão. No entanto, nenhuma nova workload pode ser associada a um perfil excluído. the section called “Notificações de perfil” são enviadas aos proprietários da workload usando perfis excluídos.

> Isenção de responsabilidade
>
> Ao compartilhar suas lentes personalizadas com outras pessoasContas da AWS, você reconhece que AWS disponibilizará suas lentes personalizadas para essas outras contas. Essas outras contas podem continuar a acessar e usar seus perfis compartilhados, mesmo que você exclua o perfil de sua própria Conta da AWS ou encerre as sua Conta da AWS.

Como excluir um perfil da lista de perfis

1. Selecione Perfis no painel de navegação à esquerda.
2. Selecione o nome do perfil que você deseja remover.
3. Escolha Excluir.
4. Para confirmar a remoção, digite o nome do perfil no campo de entrada de texto.
5. Escolha Excluir.

Se você quiser manter um perfil na sua lista de Perfis, mas removê-lo de uma workload, consulte the section called “Remover um perfil de uma workload”.

Conector da AWS Well-Architected Tool para Jira

Você pode usar o Conector da AWS Well-Architected Tool para Jira se quiser vincular sua conta do Jira ao AWS Well-Architected Tool e sincronizar itens de melhoria das workloads com projetos do Jira para ajudar a criar um mecanismo de circuito fechado na implementação de aprimoramentos.

O conector oferece sincronização automática e manual. Para ter mais detalhes, consulte Configuring the connector.

O conector pode ser configurado no nível da conta e no nível da workload, com a opção de substituir suas configurações no nível da conta por workload. No nível da workload, você também pode optar por excluir totalmente uma workload da sincronização.

Você pode optar por sincronizar os itens de melhoria com o projeto WA padrão do Jira ou especificar uma chave de projeto existente para sincronizar. No nível da workload, você pode sincronizar cada uma com um projeto exclusivo do Jira, se necessário.

> **Note**
>
> O conector só é compatível com projetos scrum e kanban no Jira.

Quando os itens de melhoria são sincronizados com o Jira, eles são organizados da seguinte forma:

- Projeto: WA (ou projeto existente que você especificar)
- Epic: workload
- Tarefa: pergunta
- Subtarefa: práticas recomendadas
- Rótulo: pilar

Depois de configurar a sincronização da conta do Jira na página Configurações, você pode configurar o conector do Jira e sincronizar itens de melhoria com sua conta do Jira.

Configurar o conector

Como instalar o conector

> **Note**
>
> Todas as etapas a seguir são executadas na sua conta do Jira, não na sua Conta da AWS.

1. Faça login na sua conta do Jira.
2. Na barra de navegação superior, escolha Apps e selecione Explore more apps.
3. Na página Discover apps and integrations for Jira, insira AWS Well-Architected. Em seguida, escolha AWS Well-Architected Tool Conector for Jira.
4. Na página do aplicativo, escolha Get app.
5. No painel Add to Jira, escolha Get it now.
6. Após a instalação do aplicativo, para concluir a configuração, escolha Configure.
7. Na página AWS Well-Architected Tool Configuration, escolha Connect a new Conta da AWS.
8. Insira a sua AccessKeyId e a chave secreta. Opcional: insira seu token de sessão. Depois, escolha Connect.

   > **Note**
   >
   > Sua conta deve ter a permissão `wellarchitected:ConfigureIntegration`. Essas permissões são necessárias para adicionar as Contas da AWS ao Jira.
   > Várias Contas da AWS podem ser conectadas ao AWS WA Tool.

   > **Note**
   >
   > Como prática recomendada de segurança, é altamente recomendável usar credenciais de curto prazo do IAM. Para ter detalhes sobre como criar um AccessKeyId e uma chave secreta para sua Conta da AWS, consulte Gerenciar chaves de acesso (console) e, para ter detalhes sobre o uso de credenciais de curto prazo, consulte Solicitar credenciais de segurança temporárias.

9. Em Regions, selecione as Regiões da AWS que você deseja conectar. Depois, escolha Connect.

Configuração do projeto do Jira

Ao usar projetos personalizados, verifique se a configuração de seu projeto tem os seguintes tipos de problema:

- Scrum: épico, história, subtarefa
- Kanban: épico, tarefa, subtarefa

Para ter detalhes sobre como gerenciar tipos de problema, consulte Atlassian Support | Add, edit, and delete an issue type.

Como verificar o status do conector no AWS Well-Architected Tool

1. Faça login na sua Conta da AWS e navegue até o AWS Well-Architected Tool.
2. Selecione Configurações no painel de navegação à esquerda.
3. Na seção Sincronização de contas no Jira, em Status da conexão do aplicativo Jira, verifique o status Configurado.

O conector agora está instalado e pronto para ser configurado. Para definir as configurações de sincronização do Jira no nível da conta e da workload, consulte Configuring the connector.

Configurar o conector do

Com o Conector da AWS Well-Architected Tool para Jira, você pode configurar a sincronização do Jira no nível da conta e da workload ou em ambos. Você pode definir as configurações do Jira no nível da workload, independentemente das configurações no nível da conta, ou substituir as configurações no nível da conta em determinada workload para especificar o respectivo comportamento de sincronização. Você também pode definir as configurações do Jira ao definir uma workload.

O conector oferece dois métodos de sincronização: automática e manual. Em ambos os métodos de sincronização, as alterações feitas no AWS WA Tool são refletidas em seu projeto do Jira, e as alterações feitas no Jira são sincronizadas novamente com o AWS WA Tool.

> **Important**
>
> Ao usar a sincronização automática, você concorda que o AWS WA Tool modifique a workload em resposta a alterações no Jira.
> Se você tiver informações confidenciais que não deseja sincronizar com o Jira, não as insira no campo Observações em suas workloads.

- Sincronização automática: o conector atualiza automaticamente seu projeto do Jira e sua workload sempre que uma pergunta é atualizada, além de selecionar ou desmarcar a seleção de uma prática recomendada e responder a uma pergunta.
- Sincronização manual: você deve escolher Sincronizar com o Jira no painel da workload quando quiser sincronizar itens de melhoria entre o Jira e o AWS WA Tool. Você também pode escolher quais perguntas e pilares específicos deseja sincronizar. Para ter mais detalhes, consulte Sincronizar uma workload.

Como configurar o conector no nível da conta

1. Selecione Configurações no painel de navegação à esquerda.
2. No painel Sincronização de contas do Jira, escolha Editar.
3. Em Tipo de sincronização, escolha uma das seguintes opções:
   a. Para sincronizar automaticamente as workloads quando as alterações forem feitas, selecione Automático.
   b. Para escolher manualmente quando sincronizar workloads, selecione Manual.
4. Por padrão, o conector cria um projeto WA do Jira. Para especificar sua própria chave do projeto do Jira, faça o seguinte:
   a. Selecione Substituir chave do projeto no Jira padrão.
   b. Insira sua chave do projeto do Jira.

   > **Note**
   >
   > A chave do projeto do Jira especificada é usada para todas as workloads, a menos que você altere o projeto no nível da workload.
5. Escolha Salvar configurações.

Como configurar o conector no nível da workload

1. Selecione Cargas de trabalho no painel de navegação à esquerda e escolha o nome da workload que você deseja configurar.
2. Escolha Properties (Propriedades).
3. No painel do Jira, escolha Editar.
4. Para definir as configurações do Jira da workload, selecione Substituir as configurações no nível da conta.

   > **Note**
   >
   > A opção Substituir as configurações do nível da conta deve estar selecionada para que as configurações específicas da workload sejam aplicadas.

5. Em Substituição de sincronização, selecione uma das seguintes opções:

   a. Para excluir a workload da sincronização do Jira, selecione Não sincronizar workload.

   b. Para escolher manualmente quando sincronizar a workload, selecione Sincronizar workload (manual).

   c. Para sincronizar as alterações da workload automaticamente, selecione Sincronizar workload (automático).

6. (Opcional) Em Chave do projeto no Jira, insira a chave do projeto com a qual sincronizar a workload. Essa chave do projeto pode ser diferente da chave do projeto no nível da conta.

   Se você não especificar uma chave de projeto, o conector criará um projeto WA do Jira.

7. Escolha Salvar.

Para ter detalhes sobre como realizar uma sincronização manual, consulte Sincronizar uma workload.

Sincronizar uma workload

No caso da sincronização automática, o conector sincroniza automaticamente os itens de melhoria quando você atualiza uma workload (por exemplo, ao responder uma pergunta ou selecionar uma nova prática recomendada).

Tanto na sincronização manual quanto na automática, todas as alterações feitas no Jira (como responder a uma pergunta ou concluir uma prática recomendada) são sincronizadas novamente com o AWS Well-Architected Tool.

Como sincronizar manualmente uma workload

1. Quando estiver tudo pronto para sincronizar a workload com o Jira, selecione Cargas de trabalho no painel de navegação à esquerda. Em seguida, selecione a workload que deseja sincronizar.
2. Na visão geral da workload, escolha Sincronizar com o Jira.
3. Selecione a lente que deseja sincronizar.
4. Em Perguntas para sincronizar com o Jira, selecione as perguntas ou os pilares completos que você deseja sincronizar com o projeto do Jira.
    - Com relação a qualquer pergunta que você queira remover, selecione o ícone X ao lado do título da pergunta.
5. Escolha Sincronizar.

Desinstalar o conector

Para desinstalar totalmente o Conector da AWS Well-Architected Tool para Jira, execute as seguintes tarefas:

- Desative a sincronização do Jira em qualquer workload que substitua as configurações de sincronização no nível da conta.
- Desative a sincronização do Jira no nível da conta.
- Desvincule sua Conta da AWS no Jira.
- Desinstale o conector da sua conta do Jira.

Como desativar o conector no nível da conta

> **Note**
>
> As seguintes etapas executadas em sua Conta da AWS:

1. Selecione Configurações no painel de navegação à esquerda.
2. Na seção Sincronização de contas no Jira, escolha Editar.
3. Desmarque a opção Ativar a sincronização de contas no Jira.
4. Escolha Salvar configurações.

Como desvincular uma Conta da AWS

> **Note**
>
> Todas as etapas a seguir são executadas na sua conta do Jira, não na sua Conta da AWS.

1. Faça login na sua conta do Jira.
2. Na barra de navegação superior, escolha Apps e selecione Manage your apps.
3. Escolha a seta suspensa ao lado de AWS Well-Architected Tool Connector for Jira e selecione Configure.
4. No painel de configuração do AWS Well-Architected Tool, para desvincular uma Conta da AWS, escolha X em Actions.

Como desinstalar o conector

> **Note**
>
> Todas as etapas a seguir são executadas na sua conta do Jira, não na sua Conta da AWS. Antes de desinstalá-lo, recomendamos verificar se todos as Contas da AWS conectadas estão desvinculadas na configuração do conector.

1. Faça login na sua conta do Jira.
2. Na barra de navegação superior, escolha Apps e selecione Manage your apps.
3. Escolha a seta suspensa ao lado de AWS Well-Architected Tool Connector for Jira.
4. Escolha Uninstall e selecione Uninstall app.

Marcos

Um marco registra o estado de uma carga de trabalho em um determinado momento.

Salve um marco depois de concluir inicialmente todas as perguntas associadas a uma carga de trabalho. À medida que a carga de trabalho é alterada com base nos itens do plano de melhoria, será possível salvar os marcos adicionais para medir o andamento.

Uma prática recomendada é salvar um marco sempre que você fizer melhorias em uma carga de trabalho.

Salvar um marco

Um marco registra o estado atual de uma carga de trabalho. O proprietário de uma carga de trabalho pode salvar um marco a qualquer momento.

Como salvar um marco

1. Na página de detalhes da carga de trabalho, selecione Save milestone (Salvar marco).
2. Na caixa Milestone name (Nome do marco), insira um nome para o marco.

   > **Note**
   >
   > O nome deve ter de 3 a 100 caracteres. Pelo menos três caracteres não devem ser espaços. Os nomes de marcos associados a uma carga de trabalho devem ser exclusivos. Os espaços e a capitalização são ignorados ao verificar a exclusividade.

3. Selecione Save (Salvar) para salvar o marco.

Depois que um marco for salvo, não será possível alterar os dados registrados da carga de trabalho. Ao excluir uma carga de trabalho, os marcos associados a ela também serão excluídos.

Visualizar marcos

É possível visualizar os marcos de uma carga de trabalho das seguintes maneiras:

- Na página de detalhes da carga de trabalho, selecione Milestones (Marcos) e escolha o marco que deseja visualizar.

- Na página Dashboard (Painel), selecione a carga e trabalho e, na seção Milestones (Marcos), escolha o marco que deseja visualizar.

Gerar um relatório de marcos

É possível gerar um relatório de marcos. O relatório contém as respostas às perguntas sobre a carga de trabalho, suas observações e todos os riscos altos e médios que estavam presentes quando o marco foi salvo.

Um relatório permite que você compartilhe detalhes sobre o marco com outras pessoas que não têm acesso ao AWS Well-Architected Tool.

Para gerar um relatório de marcos

1. Selecione o marco de uma das maneiras a seguir.
   - Na página de detalhes da carga de trabalho, selecione Milestones (Marcos) e escolha o marco.
   - Na página Dashboard (Painel), escolha a carga de trabalho com o marco sobre o qual você deseja criar um relatório. Na seção Milestones (Marcos), selecione o marco.
2. Selecione Generate report (Gerar relatório) para gerar um relatório.

   O arquivo PDF será gerado e você poderá fazer download dele ou visualizá-lo.

Compartilhar convites

Um convite de compartilhamento é uma solicitação para compartilhar uma workload, uma lente personalizada ou um modelo de avaliação pertencente a outra conta da AWS. Uma workload ou lente pode ser compartilhada com todos os usuários de uma Conta da AWS, usuários individuais ou ambos.

- Se você aceitar um convite de workload, a workload será adicionada às suas páginas de Workloads e Painel.
- Se você aceitar um convite de lente personalizada, a lente será adicionada à sua página de lentes personalizadas.
- Se você aceitar um convite de perfil, o perfil será adicionado à sua página Perfis.
- Se você aceitar um convite de modelo de avaliação, o modelo será adicionado à sua página de modelos de avaliação.

Se você rejeitar o convite, ele será removido da lista.

> **Note**
>
> Workloads, lentes personalizadas, perfis e modelos de avaliação só podem ser compartilhados na mesma Região da AWS.

O proprietário da workload controla quem tem acesso compartilhado.

A página Compartilhar convites, disponível na navegação à esquerda, fornece informações sobre sua workload pendente e convites personalizados para lentes.

As informações a seguir são exibidas para todos os convites de carga de trabalho:

Nome

O nome da workload, da lente personalizada ou do modelo de avaliação a ser compartilhado.

Tipo de recurso

O tipo de convite: Workload, Lente personalizada, Perfis ou Modelo de avaliação.

Proprietário

O ID da Conta da AWS que é proprietária da workload.

Permissão

A permissão que você receberá para a carga de trabalho.

- Somente leitura

  Fornece acesso somente de leitura à workload, às lentes personalizadas, aos perfis ou ao modelo de avaliação.

- Colaborador

  Fornece acesso de atualização a respostas e observações, e acesso somente leitura ao restante da workload. Essa permissão está disponível apenas para workloads.

Detalhes de permissões

Descrição detalhada da permissão

Aceitando um convite de compartilhamento

Para aceitar um convite de compartilhamento

1. Selecione o convite de compartilhamento a ser aceito.
2. Escolha Accept (Aceitar).

Para convites de workload, a workload é adicionada às páginas Workloads e Painel. Para convites de lentes personalizadas, a lente personalizada é adicionada à página Lentes personalizadas. Para convites de perfil, o perfil é adicionado à página Perfis. Para convites de modelos de avaliação, o modelo é adicionado à página Modelos de avaliação.

Você tem sete dias para aceitar um convite. Se você não aceitar o convite em até sete dias, ele expirará automaticamente.

Se um usuário e sua Conta da AWS tiverem aceitado convites de workload, o convite de workload para o usuário determinará a permissão do usuário.

Rejeitar um convite de compartilhamento

Para rejeitar um convite de compartilhamento

1. Selecione a workload ou o convite de lente personalizada a ser rejeitado.
2. Escolha Rejeitar.

O convite é removido da lista.

Notificações

A página Notificações exibe diferenças de versão para workloads e modelos de avaliação que têm lentes e perfis associados a eles. É possível atualizar para a versão mais recente de uma lente ou perfil para uma workload na página Notificações.

Notificações de lentes

Quando uma nova versão de uma lente estiver disponível, um banner será exibido na parte superior da página Workloads ou Modelos de avaliação para notificá-lo. Se você visualizar uma workload específica ou um modelo de avaliação usando uma lente desatualizada, também verá um banner indicando que uma nova versão da lente está disponível.

Escolha Exibir upgrades disponíveis para obter uma lista de workloads ou revisar modelos que podem ser atualizados.

Consulte the section called “Fazer upgrade de uma lente” para obter instruções sobre como atualizar uma lente para uma workload ou um modelo de avaliação.

Quando o proprietário de uma lente compartilhada a exclui, se você tiver uma workload associada à lente excluída, receberá uma notificação de que ainda poderá usar a lente na workload existente, mas não poderá adicioná-la a novas workloads.

Notificações de perfil

Há dois tipos de notificações de perfil:

- Atualização do perfil
- Exclusão de perfil

Quando um perfil associado a uma workload tiver sido editado (para obter mais informações, consulte the section called “Edição de um perfil”), uma notificação de que há uma nova versão do perfil será exibida em Notificações de perfil.

Quando o proprietário de um perfil compartilhado o exclui, se você tiver uma workload associada ao perfil excluído, receberá uma notificação de que ainda poderá usar o perfil na workload existente, mas não poderá adicioná-lo a novas workload.

Para atualizar uma versão de perfil

1. No painel de navegação à esquerda, selecione Notificações.
2. Selecione o nome da workload na lista da guia Notificações de perfil ou use a barra de pesquisa para pesquisar pelo nome da workload.
3. Escolha a versão do perfil de upgrade.
4. Na seção Confirmação, selecione a caixa de confirmação para Eu entendo e aceito essas alterações.
5. (Opcional) Se optar por salvar um marco, selecione a caixa Salvar um marco e forneça um nome para o marco.
6. Selecione Save (Salvar).

Depois que o perfil é atualizado, o número da versão mais recente e a data de atualização são exibidos na seção Perfil da workload.

Consulte Perfis Para mais informações.

Painel

O Painel, disponível na navegação à esquerda, dá acesso às suas workloads e aos problemas de médio e alto risco associados a elas. Também é possível incluir workloads que foram compartilhadas com você. O Painel é composto de quatro seções.

- Resumo: mostra o número total de workloads, quantas têm riscos altos e médios e o número total de problemas de risco alto e médio em todas as workloads.
- Problemas do Well-Architected Framework por pilar: mostra uma representação gráfica dos problemas de alto e médio risco por pilar para todas as suas workloads.
- Problemas do Well-Architected Framework por workload: mostra os problemas de alto e médio risco por pilar para cada uma das workload.
- Problemas do Well-Architected Framework por item do plano de melhoria: mostra os itens do plano de melhoria para todas as suas workloads.

Resumo

Esta seção mostra o número total de workloads e o número de workloads com problemas de risco alto e médio nas lentes do Well-Architected Framework e em todas as outras lentes. O número total de problemas de alto e médio risco em todas as workloads, pertencentes ou compartilhadas com sua Conta da AWS, é mostrado.

Escolha Incluir workloads compartilhadas comigo para que as estatísticas resumidas, o relatório consolidado e as outras seções do painel reflitam tanto as suas workloads quanto as workloads que foram compartilhadas com você.

Selecione Gerar relatório para que um relatório consolidado seja criado para você como um arquivo PDF.

O nome do relatório está no formato de: `wellarchitected_consolidatedreport_`*`account-ID`*`.pdf`.

Problemas do Well-Architected Framework por pilar

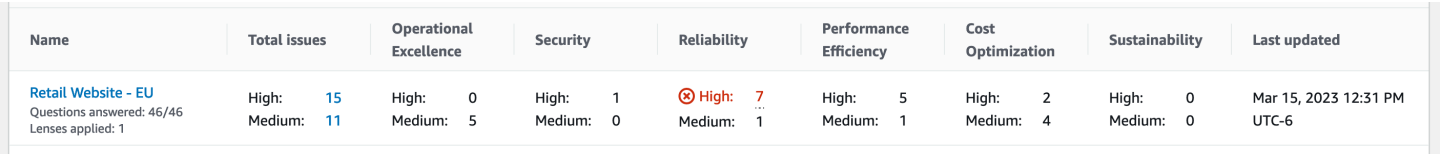
A seção Problemas do Well-Architected Framework por pilar mostra uma representação gráfica do número de problemas de alto e médio risco por pilar para todas as workloads.

Use as seções restantes do painel para passar de um nível de detalhe para o próximo.

> **Note**
>
> Somente problemas das lentes do Well-Architected Framework estão incluídos nesta seção.

Problemas do Well-Architected Framework por workload

A seção Problemas do Well-Architected Framework por workload exibe informações para cada workload.



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

As informações a seguir são exibidas para cada carga de trabalho:

Nome

O nome da carga de trabalho. O número de perguntas respondidas e o número de lentes aplicadas à workload também são mostrados.

Escolha o nome da workload para visitar a página de detalhes da workload e ver marcos, planos de melhoria e compartilhamentos.

Total de problemas

O número total de problemas identificados pelas lentes do Well-Architected Framework para a workload.

Escolha o número de problemas de alto ou médio risco para ver os planos de melhoria recomendados para esses problemas.

Excelência operacional

O número de problemas de alto risco (HRIs) e problemas de médio risco (MRIs) identificados na workload do pilar de Excelência Operacional.

Segurança

O número de HRIs e ressonâncias magnéticas identificadas para o pilar Segurança.

Confiabilidade

O número de HRIs e MRIs identificados para o pilar de confiabilidade.

Eficiência de desempenho

O número de HRIs e MRIs identificados para o pilar de Eficiência de Desempenho.

Otimização de custo

O número de HRIs e MRIs identificados para o pilar de otimização de custos.

Sustentabilidade

O número de HRIs e MRIs identificados para o pilar de Sustentabilidade.

Última atualização

Data e hora em que a carga de trabalho foi atualizada pela última vez.

Para cada workload, o pilar com o maior número de problemas de alto risco (HRIs) é destacado.

> **Note**
>
> Somente problemas das lentes do Well-Architected Framework estão incluídos nesta seção.

Problemas do Well-Architected Framework por item do plano de melhoria

A seção Problemas do Well-Architected Framework por item do plano de melhoria exibe os itens do plano de melhoria para todas as suas workloads. Você pode filtrar os itens com base no pilar e na gravidade.

As informações a seguir são exibidas para cada item do plano de melhoria:

Item de melhoria

O nome do item do plano de melhoria.

Escolha o nome para mostrar a melhor prática associada ao item do plano de melhoria.

Pilar

O pilar associado ao item de melhoria.

Risco

Indica se o problema associado é de alto ou médio risco.

Workloads aplicáveis

O número de workloads às quais esse plano de aprimoramento se aplica.

Selecione um item do plano de melhoria para ver as workloads aplicáveis.

> **Note**
>
> Somente os itens do plano de aprimoramento das lentes do Well-Architected Framework estão incluídos nesta seção.

Segurança no AWS Well-Architected Tool

A segurança na nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de data centers e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa os serviços da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Well-Architected Tool, consulte Serviços da AWS em escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o .AWS WA Tool Os tópicos a seguir mostram como configurar o AWS WA Tool para atender aos seus objetivos de segurança e conformidade. Saiba como usar outros serviços AWS que ajudam a monitorar e proteger os recursos do AWS WA Tool.

Tópicos

- Proteção de dados no AWS Well-Architected Tool
- Identity and Access Management para o AWS Well-Architected Tool
- Resposta a incidentes no AWS Well-Architected Tool
- Validação de conformidade do AWS Well-Architected Tool
- Resiliência no AWS Well-Architected Tool
- Segurança da infraestrutura no AWS Well-Architected Tool
- Análise de vulnerabilidade e configuração no AWS Well-Architected Tool
- Prevenção contra o ataque do “substituto confuso” em todos os serviços

Proteção de dados no AWS Well-Architected Tool

O AWS modelo de responsabilidade compartilhada se aplica à proteção de dados no AWS Well-Architected Tool. Conforme descrito nesse modelo, AWS é responsável por proteger a infraestrutura global que executa todas as Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da Conta da AWS e configure as contas de usuário individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure os logs de API e atividade do usuário com AWS CloudTrail. Para obter informações sobre como usar as trilhas do CloudTrail para capturar atividades da AWS, consulte Working with CloudTrail trails no Guia do usuário do AWS CloudTrail.
- Use as soluções de criptografia AWS, juntamente com todos os controles de segurança padrão em Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar a AWS por meio de uma interface de linha de comandos ou de uma API, use um endpoint do FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui trabalhar com a AWS WA Tool ou outros Serviços da AWS usando o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre

usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em repouso

Todos os dados armazenados pelo AWS WA Tool são criptografados em repouso.

Criptografia em trânsito

Todos os dados enviados de e para o AWS WA Tool são criptografados em trânsito.

Como a AWS usa seus dados

A equipe AWS Well-Architected coleta dados agregados do AWS Well-Architected Tool para fornecer e melhorar o serviço do AWS WA Tool para os clientes. Os dados individuais dos clientes podem ser compartilhados com as equipes Conta da AWS para apoiar os esforços de nossos clientes para melhorar suas workloads e arquitetura. A equipe do AWS Well-Architected só pode acessar as propriedades da workload e as opções selecionadas para cada questão. A AWS não compartilha nenhum dado do AWS WA Tool fora da AWS.

As propriedades da workload às quais a equipe do AWS Well-Architected tem acesso incluem:

- Nome da carga de trabalho
- Proprietário da revisão
- Environment
- Regiões
- IDs de conta
- Tipo de setor

A equipe AWS Well-Architected não tem acesso a:

- Descrição da carga de trabalho
- Design da arquitetura
- Qualquer nota que você inseriu

Identity and Access Management para o AWS Well-Architected Tool

AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda o administrador no controle de segurança de acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) a usar os recursos do AWS WA Tool. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

- Público
- Como autenticar com identidades
- Gerenciar o acesso usando políticas
- Como o AWS Well-Architected Tool funciona com o IAM
- Exemplos de políticas baseadas em identidade do AWS Well-Architected Tool
- Políticas gerenciadas pela AWS para o AWS Well-Architected Tool
- Solução de problemas de identidade e acesso do AWS Well-Architected Tool

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho que for realizado no AWS WA Tool.

Usuário do serviço: se você usar o serviço AWS WA Tool para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais recursos do AWS WA Tool para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no AWS WA Tool, consulte Solução de problemas de identidade e acesso do AWS Well-Architected Tool.

Administrador do serviço: se você for o responsável pelos recursos do AWS WA Tool na empresa, provavelmente terá acesso total ao AWS WA Tool. Cabe a você determinar quais funcionalidades e recursos do AWS WA Tool os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Analise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre

como a empresa pode usar o IAM com o AWS WA Tool, consulte Como o AWS Well-Architected Tool funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao AWS WA Tool. Para visualizar exemplos AWS WA Tool de políticas baseadas em identidade do que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade do AWS Well-Architected Tool.

Como autenticar com identidades

A autenticação é a forma como fazer login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como Usuário raiz da conta da AWS, como usuário do IAM, ou assumindo um perfil do IAM.

É possível fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center (Centro de Identidade do IAM), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

A depender do tipo de usuário, você pode fazer login no AWS Management Console ou no portal de acesso AWS. Para obter mais informações sobre como fazer login na AWS, consulte Como fazer login na contaConta da AWS no Início de Sessão da AWS Guia do usuário.

Se você acessar a AWS de forma programática, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comandos (CLI) para você assinar de forma criptográfica as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Usuário-raiz Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login com acesso completo a todos os Serviços da AWS e recursos na conta. Essa identidade, chamada usuário-raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha usada para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar os Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web, o AWS Directory Service, o diretório do Centro de Identidade ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. É possível criar usuários e grupos no IAM Identity Center ou conectar-se e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários

de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade na Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente um perfil do IAM no AWS Management Console, você pode alternar de um usuário para um perfil do IAM (console). É possível presumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center.
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem anexar uma política diretamente a um recurso (em vez de usar um perfil como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

- Acesso entre serviços: alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS): qualquer pessoa que utilizar um perfil ou usuário do IAM para executar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS usa as permissões da entidade principal chamando um AWS service (Serviço da AWS), bem como o AWS service (Serviço da AWS) solicitante, para fazer solicitações para serviços subsequentes. As solicitações de FAS são feitas somente quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Perfil vinculado a serviço: um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir o perfil para executar uma ação em seu nome. Perfis vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da API da AWS. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário-raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Não é possível usar as políticas gerenciadas pela AWS do IAM em uma política baseada em atributos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que oferecem compatibilidade com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS oferece compatibilidade com tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço que agrupa e gerencia centralmente várias Contas da AWS pertencentes a sua empresa. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. A SCP limita as permissões para entidades em contas de membros, o que inclui cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Service control policies no Guia do usuário do AWS Organizations.
- Políticas de controle de recursos (RCPs): RCPs são políticas JSON que podem ser usadas para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. A RCP limita as permissões para recursos nas contas-membro e pode afetar as permissões efetivas para identidades, incluindo o Usuário raiz da conta da AWS, independentemente de pertencerem a sua organização. Consulte mais informações sobre o Organizations e as RCPs, incluindo uma lista de Serviços da AWS compatível com RCPs em Resource control policies (RCPs) no Guia do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina permitir ou não uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Guia do Usuário do IAM.

Como o AWS Well-Architected Tool funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AWS WA Tool, saiba quais recursos do IAM estão disponíveis para uso com o AWS WA Tool.

recursos do IAM que você pode usar com o AWS Well-Architected Tool

Atributo do IAM	Suporte a AWS WA Tool
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para obter uma visualização de alto nível de como o AWS WA Tool e outros serviços da AWS funcionam com a maioria dos recursos do IAM, consulte AWSServiços da compatíveis com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade do AWS WA Tool

Compatível com ações de políticas: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de

permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Políticas baseadas em recursos no AWS WA Tool

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de políticas para o AWS WA Tool

Compatível com ações de políticas: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de

permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de políticas no AWS WA Tool usam o seguinte prefixo antes da ação: `wellarchitected:`. Por exemplo, para permitir que uma entidade defina uma workload, um administrador deve anexar uma política que permita ações .`wellarchitected:CreateWorkload` Da mesma forma, para impedir que uma entidade exclua workloads, um administrador pode anexar uma política que negue ações .`wellarchitected:DeleteWorkload` As declarações de política devem incluir um elemento `Action` ou AWS WA Tool. O `NotAction` define seu próprio conjunto de ações que descrevem as tarefas que podem ser executadas com esse serviço.

Para ver uma lista das ações do AWS WA Tool, consulte Ações definidas pelo AWS Well-Architected Tool na Referência de autorização do serviço.

Recursos de políticas

Compatível com recursos de políticas: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recurso do AWS WA Tool e os respectivos ARNs, consulte Resources defined by AWS Well-Architected Tool na Referência de autorização do serviço. Para saber com quais ações é possível especificar o ARN de cada recurso, consulte Ações definidas peloAWS Well-Architected Tool.

O recurso da workload do AWS WA Tool tem o seguinte ARN:

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

Para obter mais informações sobre o formato de ARNs, consulte Nomes de recursos da Amazon (ARNs)AWS e namespaces de serviços da

O ARN pode ser encontrado na página Workload properties (Propriedades da workload) de uma workload. Por exemplo, para especificar uma carga de trabalho:

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

Para especificar todas as cargas de trabalho que pertencem a uma conta específica, use o caractere curinga (*):

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

Algumas ações do AWS WA Tool, como as ações de criação e listagem de workloads, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

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

Para obter uma lista dos tipos de recursos AWS WA Tool e seus ARNs, consulte Recursos definidos por AWS Well-Architected Tool na Referência de autorização do serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS Well-Architected Tool.

Chaves de condição de políticas para AWS WA Tool

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você

especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece compatibilidade com chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

O AWS WA Tool fornece uma chave de condição específica do serviço (`wellarchitected:JiraProjectKey`) e permite o uso de algumas chaves de condição globais. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS na Referência de autorização de serviço.

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece compatibilidade com chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

ACLs no AWS WA Tool

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Autorização baseada em tags do AWS WA Tool

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos recursos da AWS. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o AWS WA Tool

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, como quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionem com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login no AWS Management Console por qualquer método, exceto nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria credenciais temporárias automaticamente. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

É possível criar credenciais temporárias manualmente usando a API AWS CLI ou AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidade principal entre serviços para o AWS WA Tool

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

O usuário ou perfil do IAM usado para executar ações na AWS é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS usa as permissões da entidade principal chamando um AWS service (Serviço da AWS), bem como o AWS service (Serviço da AWS) solicitante, para fazer solicitações para serviços subsequentes. As solicitações de FAS são feitas somente quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para AWS WA Tool

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Funções vinculadas ao serviço para o AWS WA Tool

Compatível com perfis vinculados ao serviço: Não

Um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir o perfil de executar uma ação em seu nome. Perfis vinculadas ao

serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação da função vinculada a serviço desse serviço.

Exemplos de políticas baseadas em identidade do AWS Well-Architected Tool

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS WA Tool. Eles também não podem executar tarefas usando o AWS Management Console, a AWS CLI ou uma API da AWS. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

- Práticas recomendadas de política
- Usar o console do AWS WA Tool
- Permitir que os usuários visualizem suas próprias permissões
- Conceder acesso total às workloads
- Conceder acesso somente leitura às workloads
- Acessar uma workload
- Usar uma chave de condição específica do serviço para o Conector da AWS Well-Architected Tool para Jira

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do AWS WA Tool em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS, que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis em seus Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS que são específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o console do AWS WA Tool

Para acessar o console do AWS Well-Architected Tool, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do AWS WA Tool na sua Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Para garantir que essas entidades ainda possam usar o console do AWS WA Tool, anexe também a seguinte política gerenciada pela AWS às entidades:

```
WellArchitectedConsoleReadOnlyAccess
```

Para permitir a capacidade de criar, alterar e excluir workloads, anexe a seguinte política gerenciada pela AWS às entidades:

```
WellArchitectedConsoleFullAccess
```

Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da 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": "*"
        }
    ]
}
```

Conceder acesso total às workloads

Neste exemplo, você deseja conceder a um usuário em seu acesso total Conta da AWS às suas workloads. O acesso total permite que o usuário execute todas as ações no AWS WA Tool. Esse acesso é necessário para definir, excluir, visualizar e atualizar cargas de trabalho.

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

```
}
```

Conceder acesso somente leitura às workloads

Neste exemplo, você deseja conceder a um usuário em seu acesso somente leitura Conta da AWS às suas workloads. O acesso somente leitura só permite que o usuário visualize workloads no AWS WA Tool.

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

Acessar uma workload

Neste exemplo, você deseja conceder a um usuário em seu Conta da AWSacesso somente leitura a uma de suas workloads, 99999999999955555555555566666666, na `us-west-2` Região. O ID da conta é 777788889999.

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

```
}
```

Usar uma chave de condição específica do serviço para o Conector da AWS Well-Architected Tool para Jira

Este exemplo demonstra como usar a chave de condição `wellarchitected:JiraProjectKey` específica do serviço para controlar quais projetos do Jira podem ser vinculados às workloads em sua conta.

Descrevemos abaixo os usos relevantes da chave de condição:

- **`CreateWorkload:`** quando você aplica `wellarchitected:JiraProjectKey` a `CreateWorkload`, é possível definir quais projetos personalizados do Jira podem ser vinculados a qualquer workload criada pelo usuário. Por exemplo, se um usuário tentar criar uma workload com o projeto ABC, mas a política especificar apenas o projeto PQR, a ação será negada.
- **`UpdateWorkload:`** quando você aplica `wellarchitected:JiraProjectKey` a `UpdateWorkload`, é possível definir quais projetos personalizados do Jira podem ser vinculados a essa workload específica ou a qualquer workload. Por exemplo, se um usuário tentar atualizar uma workload com o projeto ABC, mas a política especificar o projeto PQR, a ação será negada. Além disso, se o usuário tiver uma workload vinculada ao projeto PQR e tentar atualizá-la para ser vinculada ao projeto ABC, a ação será negada.
- **`UpdateGlobalSettings:`** quando você aplica `wellarchitected:JiraProjectKey` a `UpdateGlobalSettings`, é possível definir quais projetos personalizados do Jira podem ser vinculados à Conta da AWS. A configuração em nível de conta protege as workloads em sua conta que não substituem as configurações do Jira em nível de conta. Por exemplo, se um usuário tiver acesso a `UpdateGlobalSettings`, ele não poderá vincular workloads em sua conta a nenhum projeto que não esteja especificado na política.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "wellarchitected:UpdateGlobalSettings",
    "wellarchitected:CreateWorkload"
   ],
```

```
    "Resource": "*",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   },
   {
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
     "wellarchitected:UpdateWorkload"
    ],
    "Resource": "WORKLOAD_ARN",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   }
  ]
}
```

Políticas gerenciadas pela AWS para o AWS Well-Architected Tool

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para casos de uso específicos, por estarem disponíveis para uso por todos os clientes da AWS. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada por AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política estiver vinculada. É provável que a AWS atualize uma política gerenciada por AWS quando um novo AWS service (Serviço da AWS) for lançado, ou novas operações de API forem disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Política gerenciada da AWS: WellArchitectedConsoleFullAccess

É possível anexar a política `WellArchitectedConsoleFullAccess` a suas identidades do IAM.

Essa política concede o acesso total ao AWS Well-Architected Tool.

Detalhes da permissão

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

Política gerenciada da AWS: WellArchitectedConsoleReadOnlyAccess

É possível anexar a política `WellArchitectedConsoleReadOnlyAccess` às identidades do IAM.

Essa política concede acesso somente leitura ao AWS Well-Architected Tool.

Detalhes da permissão

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

Política gerenciada da AWS: AWSWellArchitectedOrganizationsServiceRolePolicy

É possível anexar a política `AWSWellArchitectedOrganizationsServiceRolePolicy` às identidades do IAM.

Essa política concede permissões administrativas no AWS Organizations necessárias para dar suporte à integração do AWS Well-Architected Tool com o Organizations. Essas permissões autorizam a conta de gerenciamento da organização a habilitar o compartilhamento de recursos com o AWS WA Tool.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `organizations:ListAWSServiceAccessForOrganization`: permite que as entidades principais verifiquem se o acesso ao serviço da AWS está habilitado para o AWS WA Tool.
- `organizations:DescribeAccount`: permite que as entidades principais recuperem informações sobre uma conta na organização.
- `organizations:DescribeOrganization`: permite que as entidades principais recuperem informações sobre uma conta na organização.
- `organizations:ListAccounts`: permite que as entidades principais recuperem a lista de contas que pertencem a uma organização.
- `organizations:ListAccountsForParent`: permite que as entidades principais recuperem a lista de contas que pertencem a uma organização de determinado nó raiz na organização.
- `organizations:ListChildren`: permite que as entidades principais recuperem a lista de contas e unidades organizacionais que pertencem a uma organização de determinado nó raiz na organização.
- `organizations:ListParents`: permite que as entidades principais recuperem a lista de pais imediatos especificada pela UO ou pela conta em uma organização.
- `organizations:ListRoots`: permite que as entidades principais recuperem a lista de todos os nós raiz de uma organização.

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

Política gerenciada pela AWS: AWSWellArchitectedDiscoveryServiceRolePolicy

É possível anexar a política `AWSWellArchitectedDiscoveryServiceRolePolicy` às identidades do IAM.

Essa política permite que o AWS Well-Architected Tool acesse serviços e recursos da AWS relacionados a recursos do AWS WA Tool.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `trustedadvisor:DescribeChecks`: lista as verificações disponíveis do Trusted Advisor.
- `trustedadvisor:DescribeCheckItems`: busca dados de verificação do Trusted Advisor, incluindo status e recursos sinalizados pelo Trusted Advisor.
- `servicecatalog:GetApplication`: busca detalhes de uma aplicação do AppRegistry.
- `servicecatalog:ListAssociatedResources`: lista os recursos associados a uma aplicação do AppRegistry.
- `cloudformation:DescribeStacks`: obtém detalhes de pilhas do AWS CloudFormation.
- `cloudformation:ListStackResources`: lista os recursos associados às pilhas do AWS CloudFormation.
- `resource-groups:ListGroupResources`: lista os recursos de um ResourceGroup.
- `tag:GetResources`: obrigatório para ListGroupResources.

- `servicecatalog:CreateAttributeGroup`: cria um grupo de atributos gerenciados pelo serviço quando necessário.
- `servicecatalog:AssociateAttributeGroup`: associa um grupo de atributos gerenciados pelo serviço a uma aplicação do AppRegistry.
- `servicecatalog:UpdateAttributeGroup`: atualiza um grupo de atributos gerenciado pelo serviço.
- `servicecatalog:DisassociateAttributeGroup`: associa um grupo de atributos gerenciados pelo serviço a um aplicativo do AppRegistry.
- `servicecatalog:DeleteAttributeGroup`: cria um grupo de atributos gerenciados pelo serviço quando necessário.

```
{
 "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-*"
   ]
  }
 ]
}
```

Atualizações do AWS WA Tool para políticas gerenciadas pela AWS

Visualizar detalhes sobre atualizações em políticas gerenciadas pela AWS para o AWS WA Tool desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed de RSS na páginaAWS WA Tool Document History (Histórico do documento).

Alteração	Descrição	Data
AWS WA Tool alterou a política gerenciada	`"wellarchitected:Export*"` Adicionado a	22 de junho de 2023

Alteração	Descrição	Data
	`WellArchitectedConsoleReadOnlyAccess` .	
O AWS WA Tool adicionou a política de perfil de serviço	Essa política permite `AWSWellArchitectedDiscoveryServiceRolePolicy` acessar AWS Well-Architected Tool serviços e recursos relacionados a AWS recursosAWS WA Tool.	3 de maio de 2023
AWS WA Tooladicionou permissões	Foi adicionada uma nova ação para conceder a permissão `ListAWSServiceAccessForOrganization` a fim de autorizar o AWS WA Tool a verificar se o acesso ao serviço da AWS está habilitado para o AWS WA Tool.	22 de julho de 2022
O AWS WA Tool iniciou o rastreamento das alterações	O AWS WA Tool começou a monitorar as alterações para as políticas gerenciadas da AWS.	22 de julho de 2022

Solução de problemas de identidade e acesso do AWS Well-Architected Tool

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o e o IAM.AWS WA Tool

Tópicos

- Não estou autorizado a realizar uma ação no AWS WA Tool

Não estou autorizado a realizar uma ação no AWS WA Tool

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. Seu administrador é a pessoa que forneceu a você suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário *mateojackson* tenta usar o console para executar a açãoDeleteWorkload, mas não tem permissões.

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

Para esse exemplo, peça ao administrador para atualizar suas políticas a fim de conceder acesso ao recurso 11112222333344445555666677778888 usando a ação `wellarchitected:DeleteWorkload`.

Resposta a incidentes no AWS Well-Architected Tool

A resposta a incidentes do AWS Well-Architected Tool é uma responsabilidade da AWS. A AWS tem uma política formal e documentada e um programa que rege a resposta a incidentes.

Problemas operacionais da AWS com grande impacto são publicados no AWS Service Health Dashboard.

As emissões operacionais também são publicadas em contas individuais por meio do AWS Health Dashboard. Para obter mais informações sobre como usar o AWS Health Dashboard, consulte AWS HealthComo usar o Guia do usuário.

Validação de conformidade do AWS Well-Architected Tool

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade e selecione o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de Conformidade da AWS.

É possível baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Baixar relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os recursos a seguir para ajudar com a conformidade:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos os Serviços da AWS estão qualificados pela HIPAA.
- Recursos de Conformidade da AWS: essa coleção de manuais e guias pode ser aplicada ao seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar recursos com regras no Guia do desenvolvedor do AWS Config: o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty: este AWS service (Serviço da AWS) detecta possíveis ameaças às suas Contas da AWS, workloads, contêineres e dados ao monitorar o ambiente em busca de atividades suspeitas e maliciosas. O GuardDuty pode ajudar você a atender a diversos requisitos de conformidade, como o PCI DSS, com o cumprimento dos requisitos de detecção de intrusões requeridos por determinadas estruturas de conformidade.
- AWS Audit Manager: este AWS service (Serviço da AWS) ajuda você a auditar continuamente o seu uso da AWS para simplificar o modo como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência no AWS Well-Architected Tool

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, altas taxas de throughput e em redes altamente redundantes. Com as Zonas de Disponibilidade, é possível projetar e operar aplicações e bancos de dados que executem o failover automaticamente entre as Zonas de Disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulteAWS Infraestrutura global.

Segurança da infraestrutura no AWS Well-Architected Tool

Por ser um serviço gerenciado, o AWS Well-Architected Tool é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança da infraestrutura, consulte Proteção de Infraestrutura em Pilar de Segurança: AWS Well-Architected Framework.

Você usa AWS WA Tool chamadas de API publicadas pela para acessarAWS o por meio da rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Análise de vulnerabilidade e configuração no AWS Well-Architected Tool

A configuração e os controles de TI são uma responsabilidade compartilhada entre a AWS e você, nosso cliente. Para obter mais informações, consulte o AWS modelo de responsabilidade compartilhada da .

Prevenção contra o ataque do “substituto confuso” em todos os serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Na AWS, a personificação entre serviços pode resultar no problema do ‘confused deputy’. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos o uso das chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` em políticas de recursos para limitar as permissões que o concede a outro serviço no recurso para o recurso. Use `aws:SourceArn` se quiser que apenas um recurso seja associado ao acesso entre serviços. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou especificar vários recursos, use a chave de condição de contexto global `aws:SourceArn` com caracteres curinga (`*`) para as partes desconhecidas do ARN. Por exemplo, .`arn:aws:wellarchitected:*:`*`123456789012`*`:*`

Se o valor de `aws:SourceArn` não contiver o ID da conta, como um ARN de bucket do Amazon S3, você deverá usar ambas as chaves de contexto de condição global para limitar as permissões.

O valor de `aws:SourceArn` deve ser uma workload ou lente.

O exemplo a seguir mostra como é possível usar as chaves de contexto de condição globais `aws:SourceArn` e `aws:SourceAccount` no AWS WA Tool para evitar o problema confused deputy.

```
{
  "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"
      }
    }
  }
}
```

Compartilhar seus recursos da AWS WA Tool

Para compartilhar um recurso que você possui, faça o seguinte:

- Ativar o compartilhamento de recursos dentro da AWS Organizations (Opcional)
- Compartilhar uma workload
- Compartilhar uma lente personalizada
- Compartilhar um perfil
- Compartilhar um modelo de avaliação

Observações

- O compartilhamento de um recurso o torna disponível para uso por entidades principais fora da Conta da AWS que criou o recurso. O compartilhamento não altera as permissões que se aplicam ao recurso na conta que o criou.
- O AWS WA Tool é um serviço regional. As entidades principais com as quais você compartilha podem acessar os compartilhamentos de recursos somente nas Regiões da AWS em que foram criadas.
- Para compartilhar recursos em uma região introduzida após 20 de março de 2019, você e a Conta da AWS compartilhada devem habilitar a região no AWS Management Console. Para obter mais informações, consulte Infraestrutura global da AWS.

Ativar o compartilhamento de recursos dentro da AWS Organizations

Quando sua conta é gerenciada pelo AWS Organizations, você pode aproveitar essa vantagem para compartilhar recursos com mais facilidade. Com ou sem Organizações, um usuário pode compartilhar com contas individuais. No entanto, se a sua conta estiver em uma organização, você poderá compartilhar com contas individuais ou com todas as contas na organização ou em uma UO sem precisar enumerar cada conta.

Para compartilhar recursos dentro de uma organização, você deve primeiro usar o console do AWS WA Tool ou a AWS Command Line Interface (AWS CLI) para habilitar o compartilhamento com o

AWS Organizations. Quando você compartilha recursos na organização, o AWS WA Tool não envia convites às entidades principais. As entidades principais da organização obtêm acesso a recursos compartilhados sem trocar convites.

Quando você ativa o compartilhamento de recursos em sua organização, o AWS WA Tool cria uma função vinculada ao serviço chamada `AWSServiceRoleForWellArchitected`. Essa função pode ser assumida apenas pelo serviço AWS WA Tool e concede ao AWS WA Tool permissão para recuperar informações sobre a organização da qual ele é membro, usando a política gerenciada da AWS `AWSWellArchitectedOrganizationsServiceRolePolicy`.

Se você não precisar mais compartilhar recursos com toda a sua organização ou UOs, poderá desativar o compartilhamento de recursos.

Requisitos

- Você pode executar essas etapas somente quando tiver feito login como entidade principal na conta de gerenciamento da organização.
- A organização deve ter todos os atributos habilitados. Para obter mais informações, consulte Enabling all features in your organization no Manual do usuário do AWS Organizations.

> **Important**
>
> Você deve ativar o compartilhamento com o AWS Organizations usando o console AWS WA Tool. Isso garante que a função vinculada ao serviço `AWSServiceRoleForWellArchitected` seja criada. Se você ativar o acesso confiável com o AWS Organizations usando o console do AWS Organizations ou o comando AWS CLI enable-aws-service-access, a função vinculada ao serviço `AWSServiceRoleForWellArchitected` não será criada e você não poderá compartilhar recursos dentro da sua organização.

Para ativar o compartilhamento de recursos em sua organização

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.

   Você deve fazer login como uma entidade principal na conta de gerenciamento da organização.
2. No painel de navegação à esquerda, escolha Configurações.

3. Escolha Ativar suporte do AWS Organizations.
4. Escolha Salvar configurações.

Para ativar o compartilhamento de recursos em sua organização

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.

   Você deve fazer login como uma entidade principal na conta de gerenciamento da organização.
2. No painel de navegação à esquerda, escolha Configurações.
3. Desmarque Ativar suporte do AWS Organizations.
4. Escolha Salvar configurações.

Marcando seus Recursos AWS WA Tool

Para ajudar no gerenciamento de recursos AWS WA Tool, você pode atribuir seus próprios metadados a cada recurso em forma de tags. Este tópico descreve as tags e como criá-las.

Conteúdo

- Conceitos Básicos de Tags
- Marcando seus Recursos
- Restrições de tag
- Trabalhando com tags usando o console
- Trabalhar com tags usando a API

Conceitos Básicos de Tags

Uma tag um rótulo atribuído a um recurso AWS. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você.

As tags permitem categorizar seus recursos AWS por finalidade, proprietário ou ambiente, por exemplo. Caso possua muitos recursos do mesmo tipo, você pode identificar rapidamente um recurso específico com base nas tags atribuídas a ele. Por exemplo, é possível definir um conjunto de tags para seus serviços AWS WA Tool para ajudá-lo a rastrear o proprietário e nível da pilha de cada serviço. Recomendamos planejar um conjunto consistente de chaves de tags para cada tipo de recurso.

Tags não são automaticamente atribuídas aos recursos. Após adicionar uma tag, você pode editar as chaves e os valores das tags ou removê-las de um recurso a qualquer momento. Caso exclua um recurso, todas as respectivas tags também serão excluídas.

As tags não têm significado semântico atrelado a AWS WA Tool e são interpretadas estritamente como string de caracteres. É possível definir o valor de uma tag em uma string vazia, mas não configurar o valor de um tag como nula. Caso adicione uma tag com a mesma chave de outra existente no recurso, o novo valor substituirá o antigo.

Você pode trabalhar com tags usando AWS Management Console, AWS CLI e API de AWS WA Tool.

Se estiver usando o AWS Identity and Access Management (IAM), você poderá controlar quais usuários da sua Conta da AWS têm permissão para criar, editar ou excluir tags.

Marcando seus Recursos

Você pode marcar recursos do AWS WA Tool novos ou existentes.

Se estiver usando o console do AWS WA Tool, você poderá aplicar tags a novos recursos quando eles forem criados ou a recursos existentes a qualquer momento. Para workloads existentes, você pode aplicar tags na guia Propriedades. Para lentes personalizadas, perfis e modelos de avaliação existentes, você pode aplicar tags na guia Visão geral.

Caso esteja usando a API AWS WA Tool, AWS CLI ou SDK AWS, é possível aplicar tags a novos recursos por meio do parâmetro `tags` na ação API relevante ou, para recursos existentes, da ação API `TagResource`. Para mais informações, consulte TagResource.

Algumas ações de criação de recursos permitem especificar tags para um recurso quando o mesmo for criado. Caso as tags não possam ser aplicadas durante a criação dos recursos, haverá falha no processo de criação de recursos. Isso garante que recursos que você pretenda marcar na criação sejam criados com as tags especificadas ou não. Caso marque recursos no momento da criação, não precisará executar scripts de marcação personalizados após a criação do recurso.

A tabela a seguir descreve os recursos AWS WA Tool que podem ser marcados com tags e aqueles que podem ser marcados na criação.

Suporte à marcação para recursos AWS WA Tool

Recurso	Compatível com tags	Compatível com a propagação de tags	Compatível com o uso de tags na criação (API AWS WA Tool, AWS CLI e SDK AWS)
Workloads do AWS WA Tool	Sim	Não	Sim
Lentes personalizadas do AWS WA Tool	Sim	Não	Sim

Recurso	Compatível com tags	Compatível com a propagação de tags	Compatível com o uso de tags na criação (API AWS WA Tool, AWS CLI e SDK AWS)
Perfis do AWS WA Tool	Sim	Não	Sim
Modelos de avaliação do AWS WA Tool	Sim	Não	Sim

Restrições de tag

As restrições básicas a seguir se aplicam a tags:

- Número máximo de tags por recurso –- 50
- Em todos os recursos, cada chave de tag deve ser exclusiva e possuir apenas um valor.
- Comprimento máximo da chave –- 128 caracteres Unicode em UTF-8
- Comprimento máximo do valor –- 256 caracteres Unicode em UTF-8
- Caso seu esquema de marcação seja usado em vários serviços e recursos AWS, lembre-se de que outros serviços podem possuir restrições em caracteres permitidos. Em geral, caracteres permitidos incluem letras, números, espaços representáveis em UTF-8 e os caracteres + - = . _ : / @.
- Chaves e valores de tags diferenciam maiúsculas de minúsculas.
- Não use `aws:`, `AWS:` ou qualquer combinação de letras maiúsculas e minúsculas como um prefixo para chaves ou valores, uma vez que as mesmas são reservadas para uso AWS. Você não pode editar nem excluir chaves ou valores de tags com esse prefixo. Tags com esse prefixo não contam em limites de tags por recurso.

Trabalhando com tags usando o console

Usando o console do AWS WA Tool, você pode gerenciar as tags associadas a recursos novos ou existentes.

Adicionar tags a um recurso individual na criação

Você pode adicionar tags aos recursos do AWS WA Tool ao criá-los.

Adicionando e excluindo tags em um recurso individual

O AWS WA Tool permite adicionar ou excluir tags associadas aos seus recursos diretamente da guia Propriedades para uma workload e da guia Visão geral para lentes personalizadas, perfis e modelos de avaliação.

Para adicionar ou excluir uma tag em uma workload

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. Na barra de navegação, selecione a região a ser usada.
3. No painel de navegação, selecione Workloads.
4. Selecione a workload a ser modificada e escolha Propriedades.
5. Na seção Tags, escolha Gerenciar tags.
6. Adicione ou exclua as tags conforme necessário.
   - Para adicionar uma tag, escolha Adicionar nova tag e preencha os campos Chave e Valor.
   - Para excluir uma tag, escolha Remove (Remover).
7. Repita esse processo para cada tag que você deseja adicionar, modificar ou excluir. Escolha Salvar para salvar as alterações.

Para adicionar ou excluir uma tag em uma lente personalizada

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. Na barra de navegação, selecione a região a ser usada.
3. No painel de navegação, escolha Lentes personalizadas.
4. Selecione o nome da lente personalizada a ser modificada.
5. Na seção Tags da guia Visão geral, escolha Gerenciar tags.
6. Adicione ou exclua as tags conforme necessário.
   - Para adicionar uma tag, escolha Adicionar nova tag e preencha os campos Chave e Valor.

- Para excluir uma tag, escolha Remove (Remover).

7. Repita esse processo para cada tag que você deseja adicionar, modificar ou excluir. Escolha Salvar para salvar as alterações.

Para adicionar ou excluir uma tag em um perfil

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. Na barra de navegação, selecione a região a ser usada.
3. No painel de navegação, escolha Perfis.
4. Selecione o nome do perfil a ser modificado.
5. Na seção Tags da guia Visão geral, escolha Gerenciar tags.
6. Adicione ou exclua as tags conforme necessário.

   - Para adicionar uma tag, escolha Adicionar nova tag e preencha os campos Chave e Valor.
   - Para excluir uma tag, escolha Remove (Remover).

7. Repita esse processo para cada tag que você deseja adicionar, modificar ou excluir. Escolha Salvar para salvar as alterações.

Para adicionar ou excluir uma tag em um modelo de avaliação

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool em https://console.aws.amazon.com/wellarchitected/.
2. Na barra de navegação, selecione a região a ser usada.
3. No painel de navegação, escolha Modelos avaliação.
4. Selecione o nome do modelo de avaliação a ser modificado.
5. Na seção Tags da guia Visão geral, escolha Gerenciar tags.
6. Adicione ou exclua as tags conforme necessário.

   - Para adicionar uma tag, escolha Adicionar nova tag e preencha os campos Chave e Valor.
   - Para excluir uma tag, escolha Remove (Remover).

7. Repita esse processo para cada tag que você deseja adicionar, modificar ou excluir. Escolha Salvar para salvar as alterações.

Trabalhar com tags usando a API

Use as seguintes operações da API do AWS WA Tool para adicionar, atualizar, listar e excluir as tags de seus recursos.

Suporte à marcação para recursos AWS WA Tool

Tarefa	Ação API
Adicione ou sobrescreva uma ou mais tags.	TagResource
Exclua uma ou mais tags.	UntagResource
Listar as etiquetas de um recurso.	ListTagsForResource

Algumas ações de criação de recursos permitem especificar tags ao criar o recurso. As ações a seguir são compatíveis com o uso de tags na criação.

Tarefa	Ação API
Criar uma workload	CreateWorkload
Importar uma nova lente	ImportLens
Criar um perfil	CreateProfile
Criar um modelo de avaliação	CreateReviewTemplate

Registrar em log chamadas de API do AWS WA Tool com o AWS CloudTrail

O AWS Well-Architected Tool é integrado a AWS CloudTrail, serviço que fornece um registro das ações realizadas por um usuário, perfil ou AWS serviço em AWS WA Tool. O CloudTrail captura todas as chamadas API para AWS WA Tool como eventos. As chamadas capturadas incluem as aquelas do AWS WA Tool console e chamadas de código para operações API da AWS WA Tool. Caso crie uma trilha, voce pode habilitar a entrega contínua de eventos CloudTrail para um bucket Amazon S3, inclusive eventos para AWS WA Tool. Mesmo que não configure uma trilha, você ainda pode visualizar os eventos mais recentes no console CloudTrail em Histórico de Eventos. Ao fazer uso das informações coletadas pelo CloudTrail, é possível determinar a solicitação feita a AWS WA Tool, o endereço IP no qual a solicitação foi feita, quem fez a solicitação e quando foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o AWS CloudTrail Guia de Usuário.

Informações do AWS WA Tool no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade no AWS WA Tool, ela é registrada em um evento do CloudTrail junto a outros eventos de serviços da AWS em Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS WA Tool, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Além disso, é possível configurar outros AWS serviços para melhor analisar e agir de acordo com dados coletados do evento nos logs CloudTrail. Para obter mais informações, consulte:

- Visão Geral para Criar uma Trilha
- Serviços e integrações com suporte no CloudTrail
- Configurando Notificações Amazon SNS para CloudTrail

- Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas

Todas as ações do AWS WA Tool são registradas pelo CloudTrail e documentadas em Ações definidas pelo AWS Well-Architected Tool. Por exemplo, as chamadas para as APIs `CreateWorkload`, `DeleteWorkload` e `CreateWorkloadShare` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário ou de usuário-raiz.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para mais informações, consulte Elemento userIdentity CloudTrail.

Noções básicas sobre entradas de arquivos de log do AWS WA Tool

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket Amazon S3 especificado. Os arquivos de log CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros da solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto, não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log CloudTrail que demonstra a `CreateWorkload` ação.

```
   {
    "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

O AWS Well-Architected Tool envia eventos para o Amazon EventBridge quando ações são realizadas em recursos do Well-Architected. É possível usar o EventBridge e esses eventos para escrever regras que executam ações, como notificar você, quando ocorre uma alteração de recurso. Para obter mais informações, consulte O que é o Amazon EventBridge?

> **Note**
>
> Os eventos são entregues com base no melhor esforço.

As ações a seguir resultam em eventos do EventBridge:

- Relacionado à workload
  - Criar ou excluir uma workload
  - Criar um marco
  - Atualizar as propriedades de uma workload
  - Compartilhar ou cancelar o compartilhamento de uma workload
  - Atualizar o status de um convite de compartilhamento
  - Adicionar ou remover tags
  - Atualizar uma resposta
  - Atualizar notas de revisão
  - Adicionar ou remover uma lente de uma workload
- Relacionado à lente
  - Importar ou exportar uma lente personalizada
  - Publicar uma lente personalizada
  - Excluir uma lente personalizada
  - Compartilhar ou cancelar o compartilhamento de uma lente personalizada
  - Atualizar o status de um convite de compartilhamento
  - Adicionar ou remover uma lente de uma workload

Exemplo de eventos do AWS WA Tool

Esta seção inclui exemplos de eventos do AWS Well-Architected Tool.

Atualizar uma resposta em uma workload


```
{
  "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"
   }
}
```


Publicar uma lente personalizada


```
{
   "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"
   }
}
```

Histórico do documento

A tabela a seguir descreve a documentação desta versão do AWS Well-Architected Tool.

- Versão da API: mais recente
- Última atualização da documentação: 17 de abril de 2025

Alteração	Descrição	Data
Nova lente	Esta versão adicionou uma nova lente ao Catálogo de Lentes.	17 de abril de 2025
Lentes novas e atualizadas	Esta versão adicionou uma nova lente ao Catálogo de Lentes e atualizou outras lentes.	27 de junho de 2024
Jira	Essa versão adicionou o Conector da AWS Well-Arch itected Tool para Jira.	16 de abril de 2024
Novas lentes	Esta versão adicionou novas lentes ao Catálogo de Lentes.	26 de março de 2024
Funcionalidade atualizada	Esta versão adiciona o recurso Catálogo de lentes ao AWS WA Tool.	26 de novembro de 2023
Funcionalidade atualizada	Essa versão adiciona o recurso de modelos de avaliação ao AWS WA Tool.	3 de outubro de 2023
Política gerenciada WellArchi tectedConsoleReadO nlyAccess atualizada	`"wellarchitected:E xportLens"` Adicionado a `WellArchitectedCon soleReadOnlyAccess` .	22 de junho de 2023

Funcionalidade atualizada	Essa versão adiciona o recurso de perfis ao AWS WA Tool.	13 de junho de 2023
Funcionalidade atualizada	Essa versão aprimora a integração entre o AWS Trusted Advisor e o AWS Service Catalog AppRegistry e adiciona a `AWSWellArchitectedDiscoveryServiceRolePolicy` às políticas gerenciadas pela AWS.	3 de maio de 2023
Atualização de conteúdo	Página do Painel atualizada para incluir informações detalhadas sobre riscos e planos de melhoria. A capacidade de criar um relatório de workload consolidado também foi adicionada.	30 de março de 2023
Atualização de conteúdo	Nome corrigido da política WellArchitectedConsoleReadOnlyAccess.	19 de janeiro de 2023
Atualização da orientação do IAM para o AWS WA Tool	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	4 de janeiro de 2023
Funcionalidade atualizada	Essa versão remove a lente do FTR da ferramenta.	14 de dezembro de 2022

Funcionalidade atualizada	Esta versão adiciona a integração entre o AWS Trusted Advisor e o AWS Service Catalog AppRegistry.	7 de novembro de 2022
Atualização de conteúdo	Correção de um problema na lente personalizada do exemplo de JSON para `choices`.	29 de setembro de 2022
Atualização de conteúdo	A seção `choices` da especificação JSON da lente personalizada foi atualizada.	2 de agosto de 2022
Funcionalidade atualizada	Essa versão adiciona rastreamento de alterações para suas políticas gerenciadas da AWS e adicionou uma nova ação para conceder a permissão `ListAWSServiceAccessForOrganization` à `AWSWellArchitectedOrganizationsServiceRolePolicy`.	22 de julho de 2022
Compartilhamento de organização adicionado	Essa versão permite compartilhar workloads e lentes personalizadas com uma organização e unidades organizacionais (UOs).	30 de junho de 2022

Funcionalidade atualizada	Essa versão permite especificar recursos adicionais para opções em uma lente personalizada, de pré-visualizar uma lente personalizada antes de publicá-la e de adicionar tags às lentes personalizadas.	21 de junho de 2022
Funcionalidade atualizada	Esta versão adiciona a capacidade de acessar a comunidade do AWS Well-Architected no re:Post da AWS.	31 de maio de 2022
Funcionalidade atualizada	Essa versão adiciona o pilar de sustentabilidade e pequenas atualizações ao Tutorial.	31 de março de 2022
Suporte adicionado ao EventBridge	O AWS WA Tool agora envia um evento para o Amazon EventBridge quando uma alteração é feita em um recurso do Well-Architected.	3 de março de 2022
Funcionalidade atualizada	As práticas recomendadas individuais agora podem ser marcadas como não aplicáveis.	14 de julho de 2021
Marcação de recursos disponível	Essa versão permite adicionar tags às workloads.	3 de março de 2021
API já disponível	Essa versão adiciona a API do AWS WA Tool. Adicionadas informações de registro em log do AWS CloudTrail.	16 de dezembro de 2020

Funcionalidade atualizada	Essa versão adiciona a lente do FTR e SaaS à ferramenta.	3 de dezembro de 2020
Proteção de dados atualizada	Informações sobre proteção de dados atualizadas.	5 de novembro de 2020
Atualização de conteúdo	Esclareceu que depois de atualizar uma workload para usar uma nova lente, você não pode voltar para a versão anterior.	8 de julho de 2020
Atualização de conteúdo	Esclarecimento do compartilhamento em Regiões da AWS introduzido após 20 de março de 2019.	24 de junho de 2020
Funcionalidade atualizada	O acesso a um compartilhamento de workload é removido imediatamente quando um convite de compartilhamento de workload é rejeitado. O acesso compartilhado é concedido quando o compartilhamento é aceito.	17 de junho de 2020
Atualização de conteúdo	Adicionadas definições para problemas de alto risco (HRI) e problemas de risco médio (MRI).	12 de junho de 2020
Atualização de conteúdo	Seção adicionada sobre como a AWS usa seus dados.	21 de maio de 2020
Funcionalidade atualizada	Essa versão adiciona um proprietário de revisão à workload.	1 de abril de 2020

Funcionalidade atualizada	Esta versão adiciona um link de diagrama de arquitetura à workload.	10 de março de 2020
Atualização de conteúdo	Esclarecimento de que os compartilhamentos de workload são específicos da Região da AWS.	10 de janeiro de 2020
Funcionalidade atualizada	Esta versão inclui o compartilhamento de workload.	9 de janeiro de 2020
Atualização de conteúdo	Seção de segurança atualizada com as últimas orientações.	6 de dezembro de 2019
Funcionalidade atualizada	Esta versão torna os campos do setor opcionais ao definir uma workload.	19 de agosto de 2019
Funcionalidade atualizada	Esta versão adiciona itens de plano de melhoria ao relatório da workload.	29 de julho de 2019
Funcionalidade atualizada	A versão adiciona a ação DeleteWorkload à política.	18 de julho de 2019
Atualização de conteúdo	O conteúdo deste guia foi atualizado com pequenas correções.	19 de junho de 2019
Atualização de conteúdo	O conteúdo deste guia foi atualizado com pequenas correções.	30 de maio de 2019
Funcionalidade atualizada	Esta versão oferece suporte à atualização da versão da estrutura usada para uma avaliação de workload.	1º de maio de 2019

Funcionalidade atualizada	Essa versão permite especificar não Regiões da AWS ao definir uma workload.	14 de fevereiro de 2019
Disponibilidade geral do AWS Well-Architected Tool	Esta versão apresenta o AWS Well-Architected Tool.	29 de novembro de 2018

Glossário da AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.