Manual do usuário

AWS Well-Architected Tool

AWS Well-Architected Tool: Manual do usuário

Table of Contents

Você pode usar o AWS Well-Architected Tool Connector for Jira para vincular sua conta do Jira e sincronizar itens de melhoria entre suas cargas de trabalho e projetos do Jira. AWS Well-Architected Tool

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.

O que é o AWS Well-Architected Tool?

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

- 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 sua carga de trabalho 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 sua carga de trabalho 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 AWS.

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

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

A AWS Well-Architected Framework

A 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. A estrutura 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 melhores práticas 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, consulte AWSsite do AWS Well-Architected.

Definições

No 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 lentes 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).

Começando com AWS Well-Architected Tool

Esta seção descreve como começar com AWS WA Tool.

Tópicos

Fornecendo aos usuários, grupos ou funções acesso ao AWS WA Tool

Nesta etapa, você concede acesso AWS WA Tool a.

Forneça acesso a AWS WA Tool

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

   - Usuários e grupos em 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 Criar 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 o diretor execute todas as ações em 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 AWS políticas gerenciadas para AWS Well-Architected Tool.

Ativando o suporte para outros serviços AWS

A ativação do acesso à organização permite coletar informações sobre AWS WA Tool 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 de AWS Trusted AdvisorAWS Service Catalog AppRegistry, e recursos relacionados (como AWS CloudFormation pilhas em coleções de AppRegistry recursos) para ajudá-lo a descobrir mais facilmente as informações necessárias para responder às perguntas de revisão do Well-Architected e personalizar as verificações para uma carga de trabalho. Trusted Advisor

Ativar o suporte ou ativar o suporte do Discovery cria automaticamente uma função vinculada ao serviço para sua conta. AWS Organizations

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

1. Para coletar informações de AWS Organizations, ative Ativar AWS Organizations suporte.
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.

Ativando AppRegistry para uma carga de trabalho

AppRegistry O uso é opcional, e os clientes do AWS Business and Enterprise Support podem ativá-lo por carga de trabalho.

Sempre que o suporte ao Discovery AppRegistry é ativado e associado a uma carga de trabalho nova ou existente, AWS WA Tool cria um grupo de atributos gerenciados pelo serviço. O grupo de atributos Metadata AppRegistry contém o ARN da carga de trabalho, o nome da carga de trabalho e os riscos associados à carga de trabalho.

- 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.

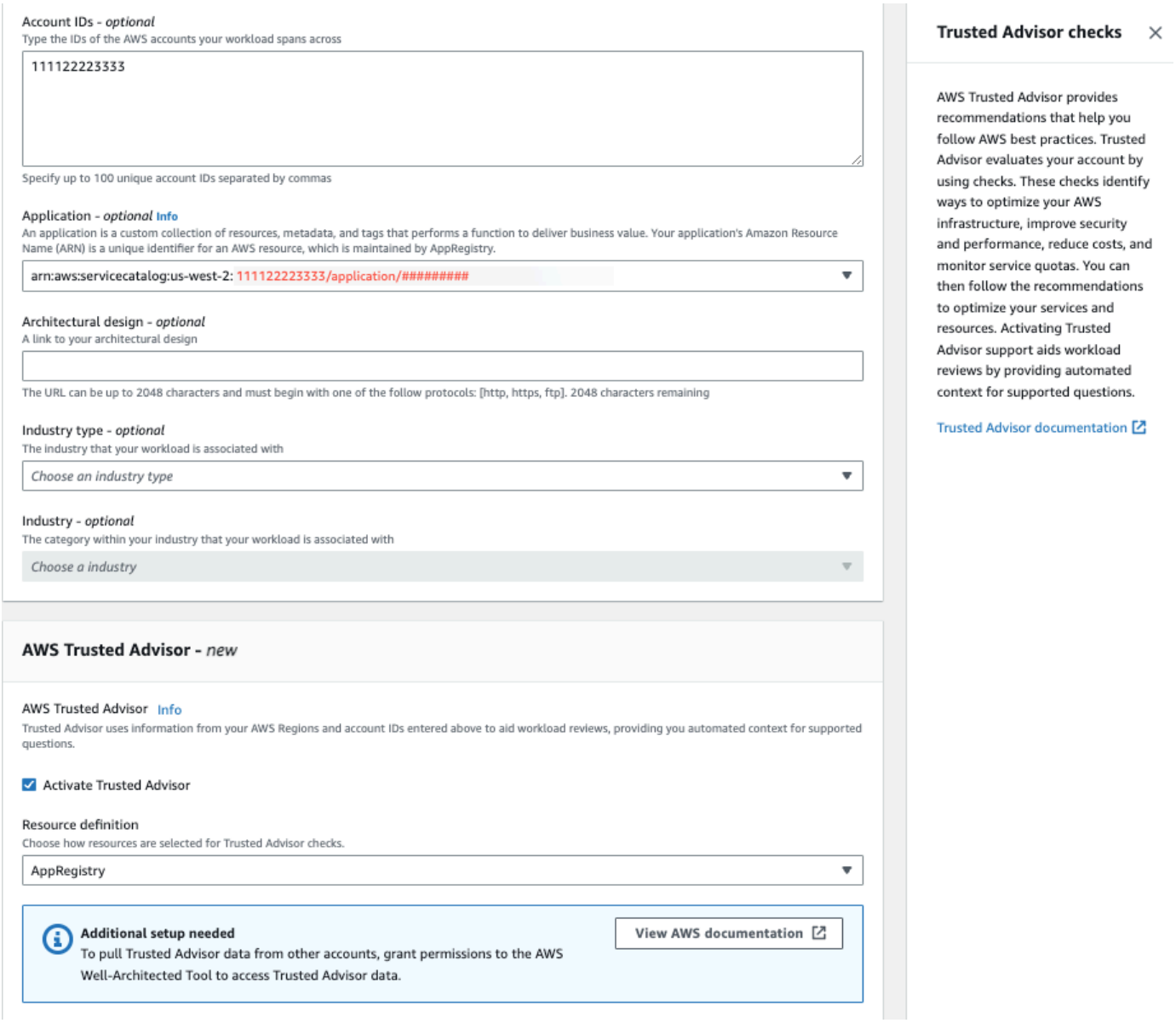
Se você quiser que um AppRegistry aplicativo conduza os dados obtidos Trusted Advisor, defina sua definição de recursos de carga de trabalho como AppRegistryou Todos. Crie funções para todas as contas que possuem recursos em seu aplicativo seguindo as diretrizes em the section called “Ativando Trusted Advisor no IAM”.

Ativando AWS Trusted Advisor para uma carga de trabalho

A integração com AWS Trusted Advisor é opcional e pode ser ativada por carga de trabalho para clientes do AWS Business e do Enterprise Support. A integração Trusted Advisor não tem custo AWS WA Tool, mas para obter detalhes sobre Trusted Advisor preços, consulte AWS Support Plans.

Para ativar o Trusted Advisor para uma workload

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



4. Uma notificação de que a função de serviço do IAM será criada é exibida na primeira vez em que Trusted Advisor é ativada para uma carga de trabalho. 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 recursos, você pode selecionar Metadados da carga de trabalho ou Tudo. AppRegistry A seleção da definição de recursos define de quais dados são AWS WA Tool buscados Trusted Advisor para fornecer as verificações de status na revisão da carga de trabalho que são mapeadas de acordo com as melhores práticas da Well-Architected.

Metadados da carga de trabalho — a carga de trabalho é definida por IDs de conta e Regiões da AWS especificada na carga de trabalho.

AppRegistry— a carga de trabalho é definida pelos recursos (como AWS CloudFormation pilhas) que estão presentes no AppRegistry aplicativo associado à carga de trabalho.

Tudo — a carga de trabalho é definida pelos metadados e pelos recursos da carga de trabalho. AppRegistry

6. Escolha Próximo.
7. Aplique o AWS Well-Architected Framework à sua carga de trabalho e escolha Definir carga de trabalho. Trusted Advisor as verificações são vinculadas apenas ao AWS Well-Architected Framework e não a outras lentes.

AWS WA Tool Periodicamente, obtém dados Trusted Advisor usando as funções criadas 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, não será AWS WA Tool possível obter Trusted Advisor informações para essa conta e exibirá um erro.

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

Ativando Trusted Advisor para uma carga de trabalho no IAM

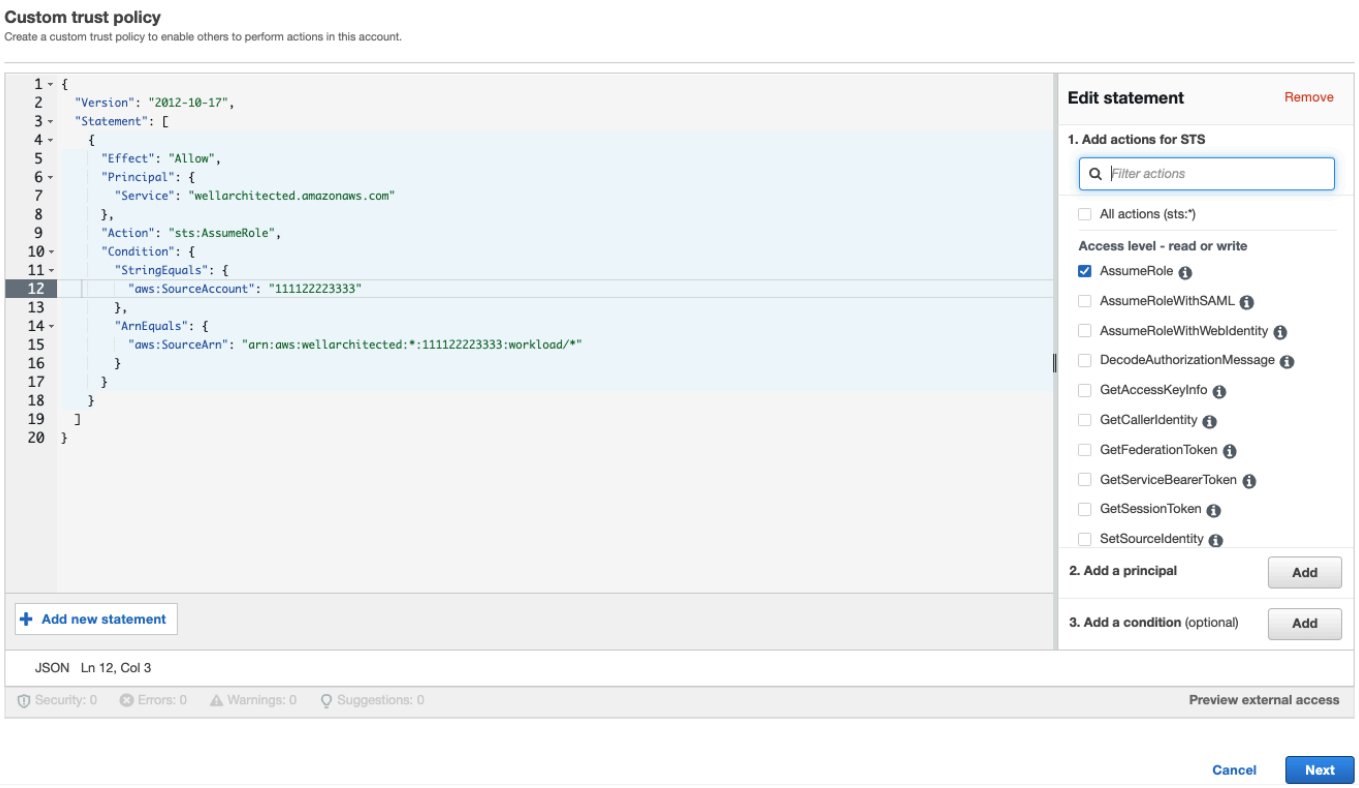
> **Note**
>
> Os proprietários da carga de trabalho devem ativar o suporte do Discovery para sua conta antes de criar uma carga Trusted Advisor de trabalho. A escolha de ativar o suporte do Discovery cria a função necessária para o proprietário da workload. Use as etapas a seguir para todas as outras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

Os proprietários das contas associadas às cargas de trabalho que foram ativadas Trusted Advisor devem criar uma função no IAM para ver Trusted Advisor as informações em AWS WA Tool.

Para criar uma função no IAM AWS WA Tool para obter informações de Trusted Advisor

1. Faça login no AWS Management Console e abra o console do IAM emhttps://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` bloco condicional da política de confiança personalizada anterior é`"arn:aws:wellarchitected:*:`*WORKLOAD_OWNER_ACCOUNT_ID*`:workload/*"`, que é uma condição genérica que indica que essa função pode ser usada AWS WA Tool para todas as cargas de trabalho do proprietário da carga de trabalho. 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 AWS WA Tool acesso à leitura de dados 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 Trusted Advisor estiver ativado para uma carga de trabalho e a definição do recurso estiver definida como AppRegistryou Todas, todas as contas que possuem um recurso no AppRegistry aplicativo anexado à carga de trabalho devem adicionar a seguinte permissão à política de permissões da Trusted Advisor função.

```
{
    "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. Selecione Next: Review (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.

Desativando Trusted Advisor para uma carga de trabalho

Para ativar o Trusted Advisor para uma workload

Você pode desativar qualquer carga Trusted Advisor de trabalho do editando sua carga de trabalho e AWS WA Tool desmarcando Ativar. Trusted Advisor Para obter mais informações sobre a edição de workloads, consulte the section called “Editar uma carga de trabalho”.

A desativação Trusted Advisor do AWS WA Tool não exclui as funções criadas no IAM. A exclusão de perfis do IAM exige uma medida de limpeza separada. Os proprietários da carga de trabalho ou proprietários de contas associadas devem excluir as funções do IAM criadas quando Trusted Advisor são desativadas AWS WA Tool ou parar AWS WA Tool de coletar Trusted Advisor dados para a carga de trabalho.

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

A próxima etapa é definir uma carga de trabalho.

Como definir uma carga de trabalho

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console em https://console.aws.amazon.com/wellarchitected/.
2. Se esta é sua primeira vez usando AWS WA Tool, você verá uma página que apresenta 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 AWS usa seus dados de carga de trabalho, escolha Por que 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 Regiões da AWS onde sua carga de trabalho é executada, uma de cada vez.
- Não AWS regiões — insira os nomes das regiões fora de AWS onde sua carga de trabalho 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 Trusted Advisor estiver ativado, todos os IDs de conta especificados serão usados para obter dados Trusted Advisor. Consulte Ativação AWS Trusted Advisor de uma carga de trabalho para conceder AWS WA Tool permissões para obter Trusted Advisor dados 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 “Ativando Trusted Advisor” para conceder AWS WA Tool permissões para obter Trusted Advisor dados em seu nome. Selecione Metadados da carga de trabalho ou Tudo em Definição de recursos para definir quais recursos são AWS WA Tool usados para executar Trusted Advisor verificações. AppRegistry
14. (Opcional) Na seção Jira, para ativar as configurações de sincronização do Jira em nível de carga de trabalho para a carga de trabalho, selecione Substituir configurações em nível de conta. Pode ser necessária uma configuração adicional para as contas associadas à sua workload. Consulte AWS Well-Architected Tool Connector for Jira para começar a instalar e configurar o conector. Selecione entre Não sincronizar carga de trabalho, Sincronizar carga de trabalho - Manual e Sincronizar carga de trabalho - Automático e, opcionalmente, insira uma chave de projeto do Jira para sincronizar.

> **Note**
>
> Se você não substituir as configurações no nível da conta, as cargas de trabalho 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 Marcar recursos do 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 AWS lentes oficiais, consulte Lentes.

    As lentes podem ser selecionadas entre lentes personalizadas (lentes que você criou ou que foram compartilhadas com você Conta da AWS), catálogo de lentes (lentes AWS oficiais 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 AWS usuário ou conta, você reconhece que lentes personalizadas criadas por outros usuários e compartilhadas com você são Conteúdo de Terceiros, conforme definido no Contrato do AWS Cliente.

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

Depois que uma carga de trabalho é definida, documente seu estado.

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.

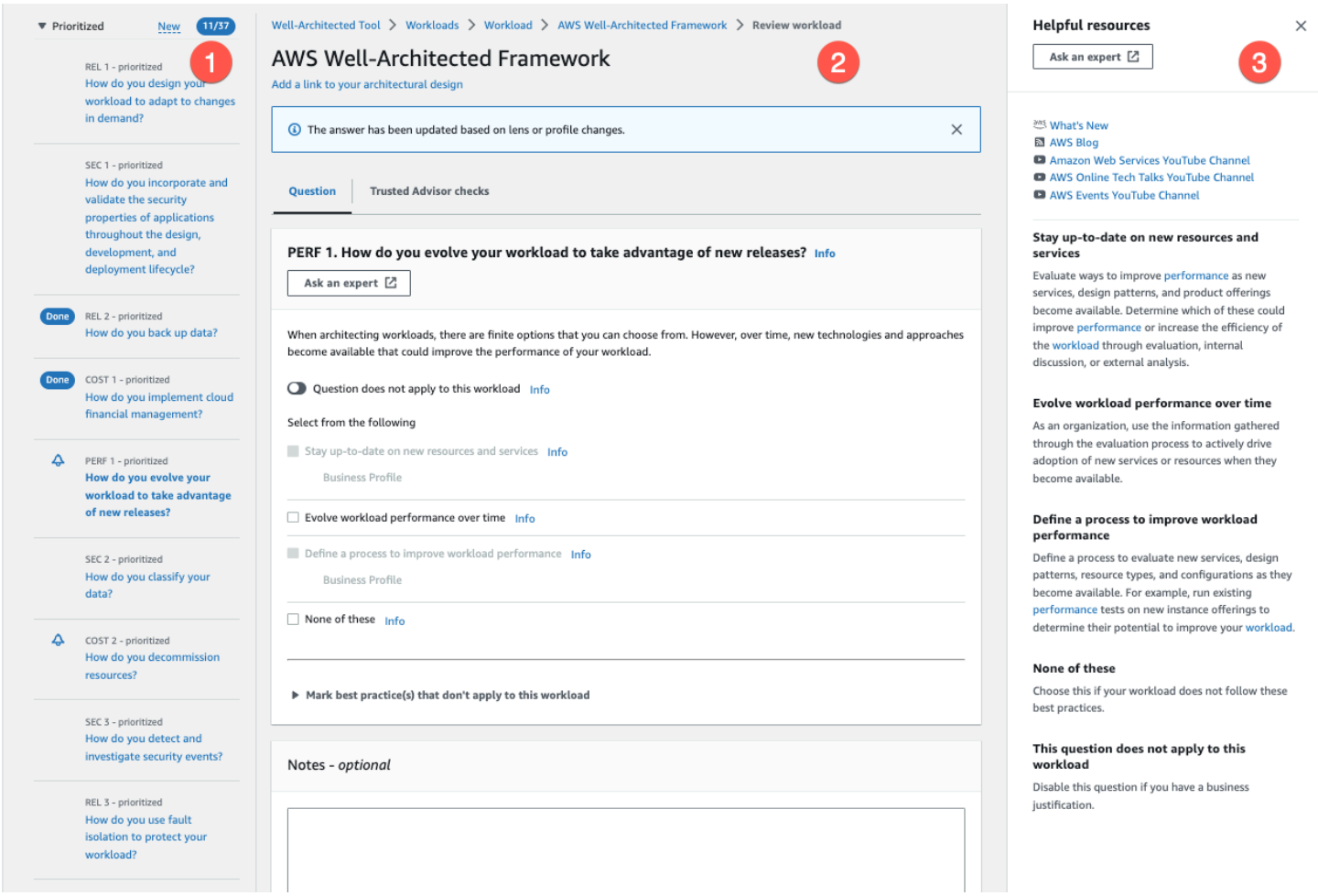
Repita essas etapas para cada pergunta em cada pilar.

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

Para retornar às perguntas, acesse a página de detalhes da carga de trabalho e selecione Continue reviewing (Continuar a revisão).

Página Revisar workload

A página de análise da workload tem três painéis.



1. 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.

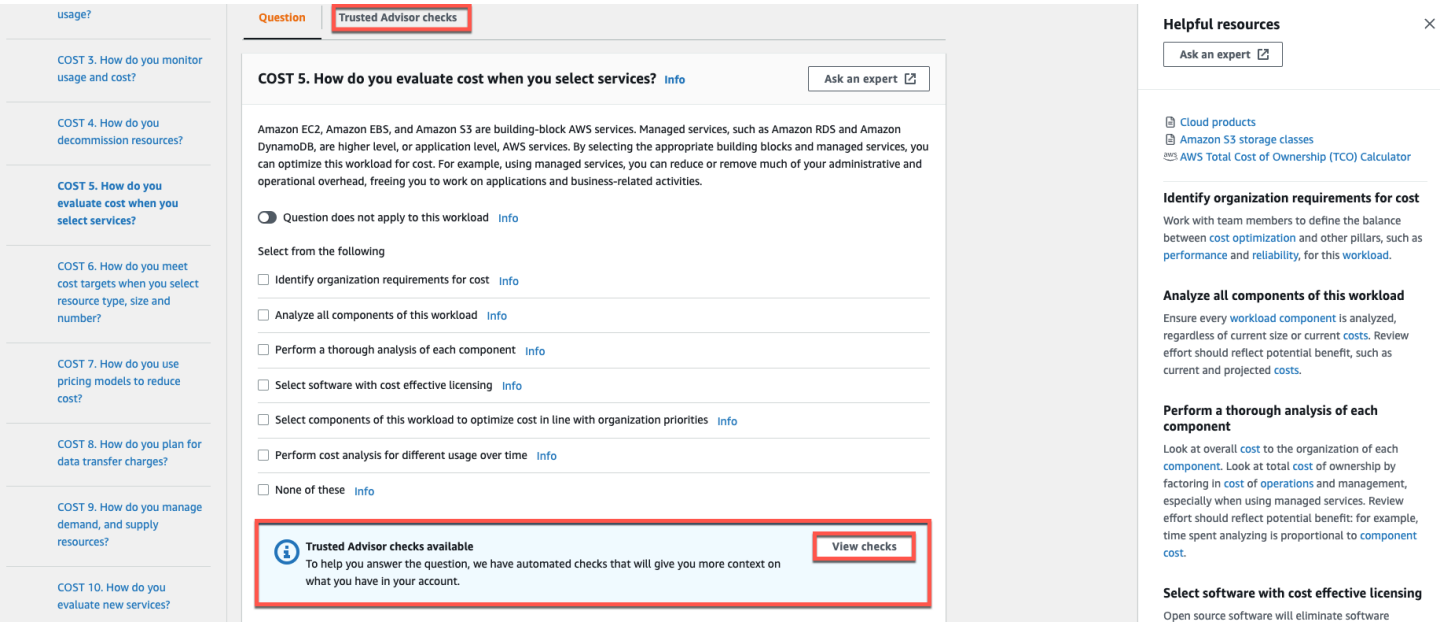
   (Opcional) Se um perfil estiver associado à sua workload, AWS WA Tool usa as informações do perfil para determinar quais perguntas na análise da workload são priorizadas e quais perguntas não são aplicáveis à sua empresa. No painel de navegação esquerdo, você pode usar as perguntas priorizadas para ajudar 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. AWS O re:post é um substituto question-and-answer comunitário baseado em tópicos para fóruns. 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.

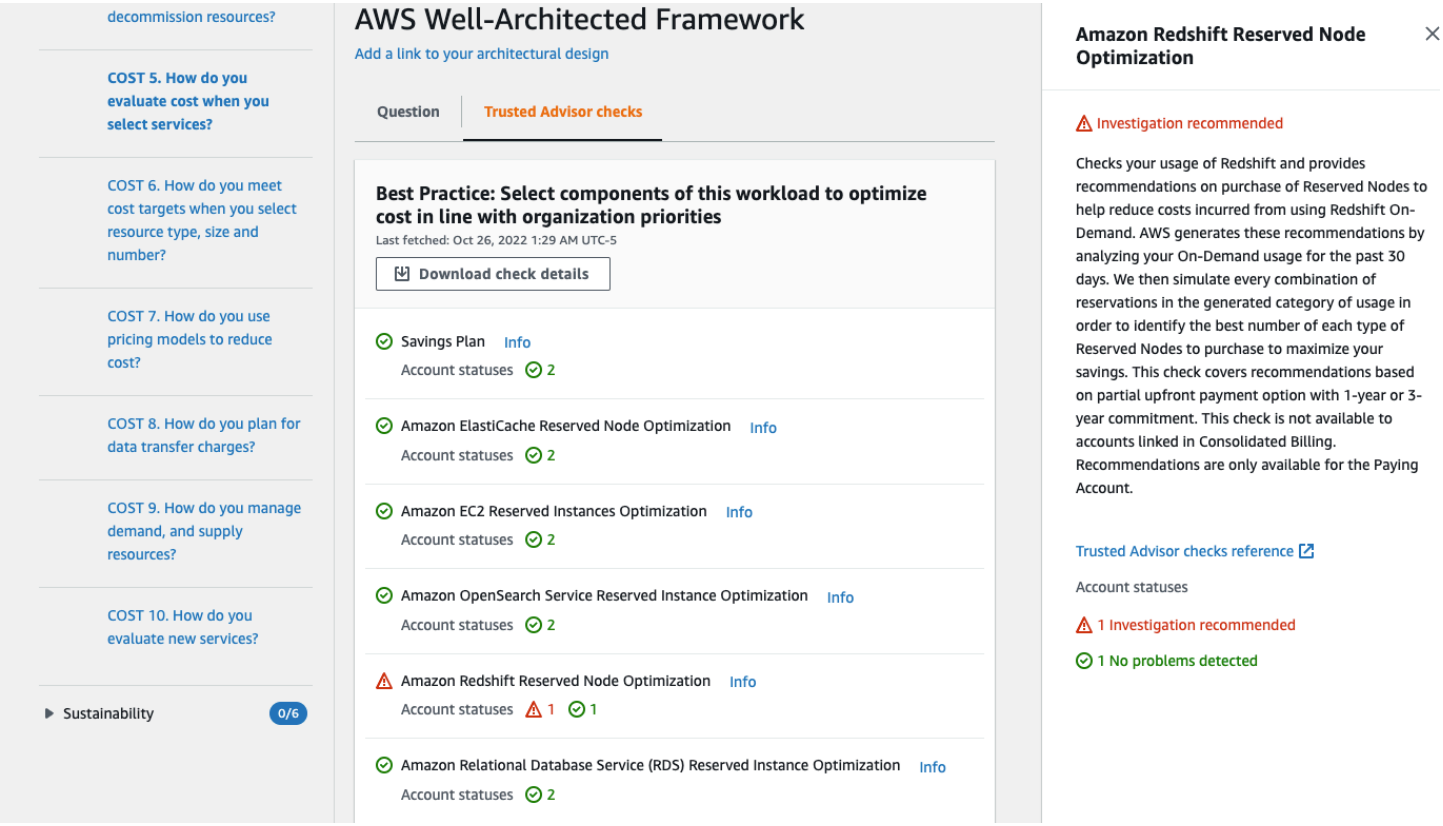
   Use os botões na parte inferior desse painel para ir para a próxima pergunta, retornar à pergunta anterior ou salvar suas alterações e sair.
3. O painel de ajuda à direita exibe informações adicionais e recursos úteis. Escolha Pergunte a um especialista para acessar a comunidade AWS re:POST dedicada ao AWS Well-Architected. Nessa comunidade, você pode fazer perguntas relacionadas ao projeto, à criação, à implantação e à operação de workloads na AWS.

Trusted Advisor cheques

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



Na guia Trusted Advisor verificações, você pode ver informações mais detalhadas sobre as verificações de melhores práticas Trusted 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 verificação 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) — Trusted Advisor recomenda uma ação para a verificação.
- Investigação recomendada (amarelo) — Trusted Advisor detecta um possível problema na verificação.
- Nenhum problema detectado (verde) — Trusted Advisor não detecta um problema na 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 AWS Support do usuário.

Selecionar o link Informações ao lado de cada Trusted Advisor verificação 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 AWS Support .

Salvar um marco

Você pode salvar um marco 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 carga de trabalho capturados naquele marco.

Para ter mais informações, consulte Marcos.

Tutorial

Este tutorial descreve o uso 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

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 carga de trabalho”.

Como definir uma carga de trabalho

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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.

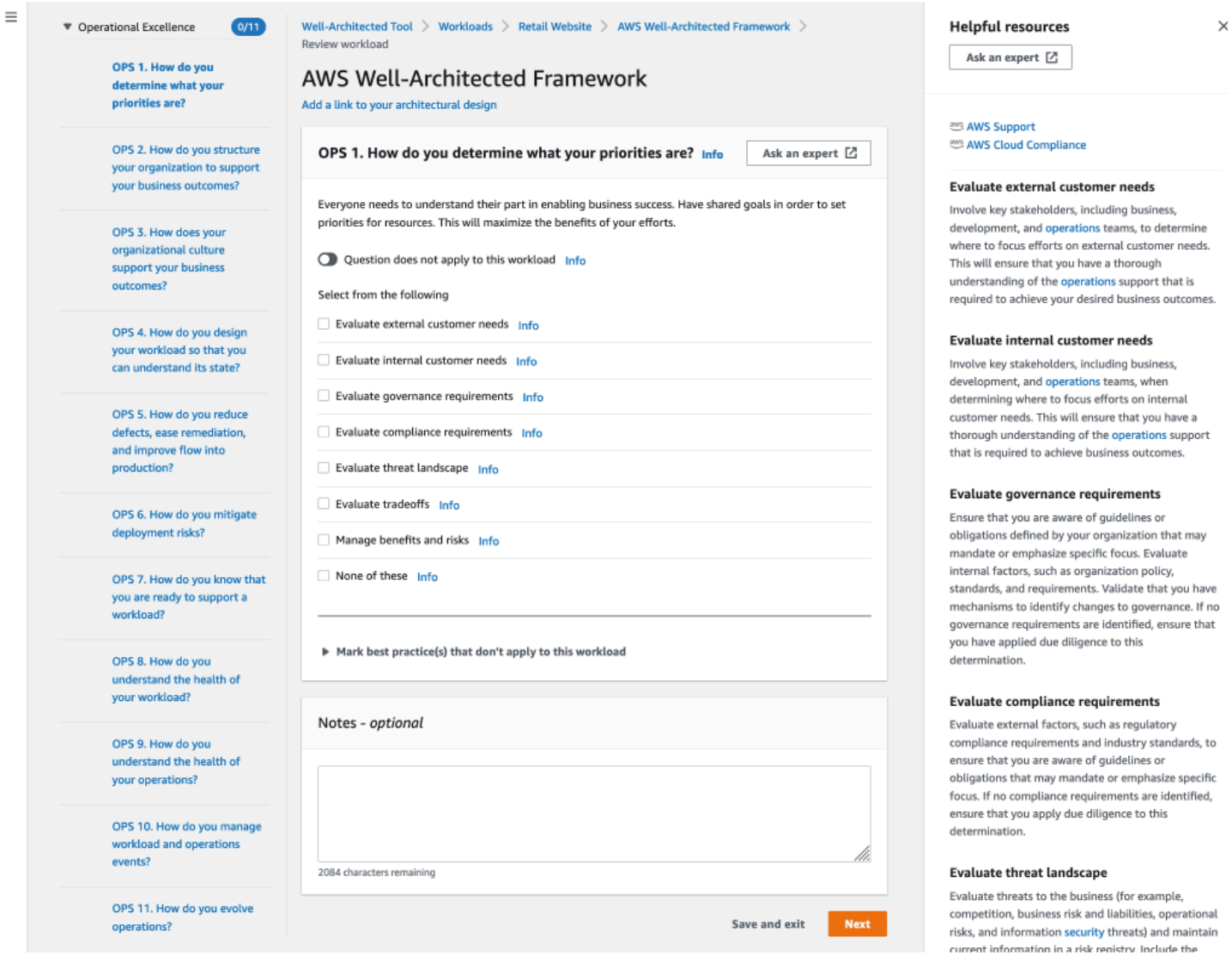
6. Na caixa Ambiente, indicamos que a workload está em um ambiente de produção.
7. Nossa carga de trabalho é executada em nosso data center local AWS e em ambos:
    a. Escolha Regiões da AWS e selecione as duas regiões na América do Norte onde a workload é executada.
    b. Selecione também Não AWS regiões 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 substitua as configurações do nível da conta na seção Jira para essa carga de trabalho.
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. Neste exemplo, aplique a lente AWS Well-Architected Framework, que é selecionada 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 carga de trabalho, você recebe perguntas para a lente selecionada que abrangem os pilares do AWS Well-Architected Framework: excelência operacional, segurança, confiabilidade, eficiência de desempenho, otimização de custos e sustentabilidade.

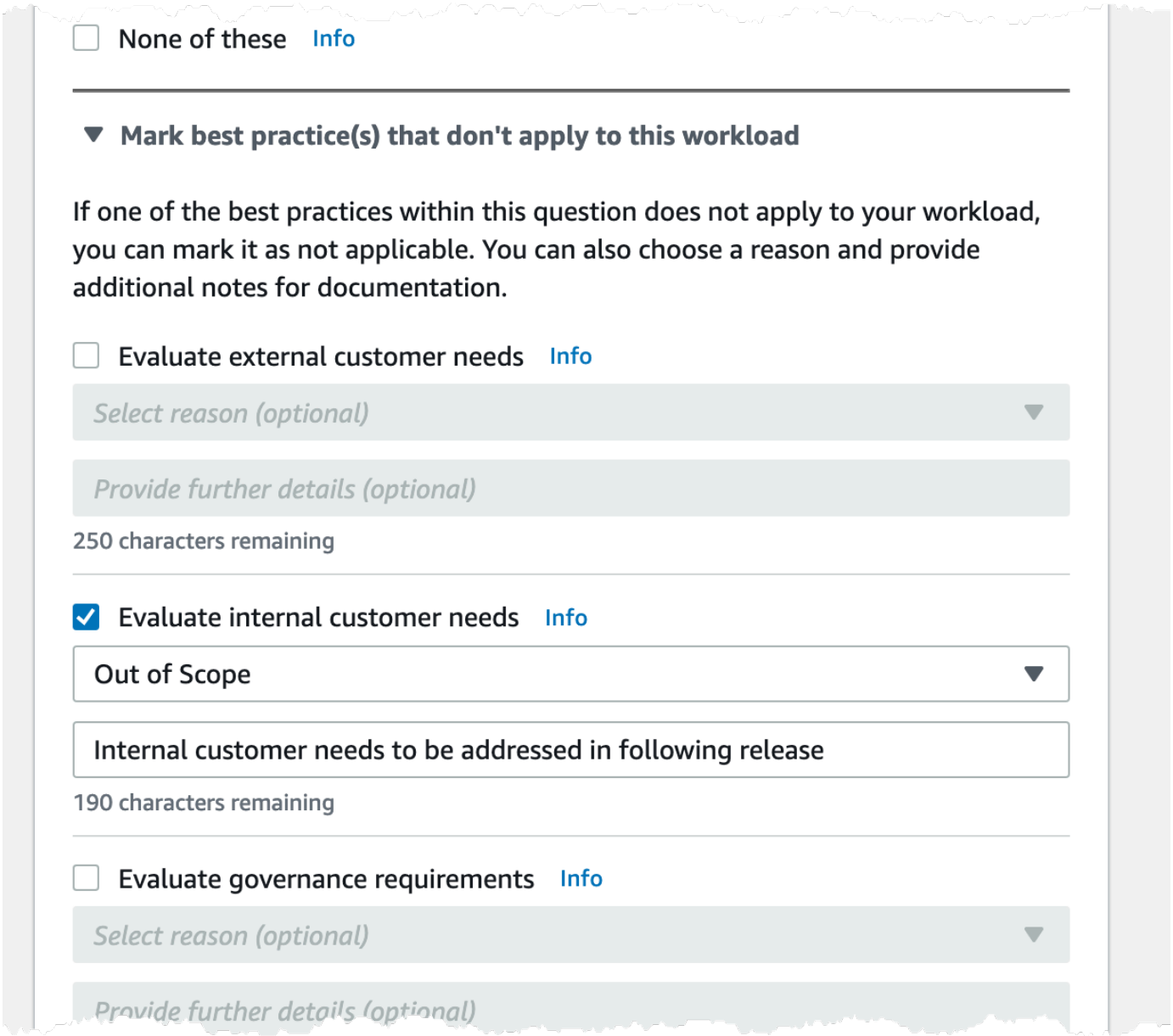
Para cada pergunta, escolha as melhores práticas que você está seguindo na lista fornecida. Se precisar de detalhes sobre uma prática recomendada, selecione Info (Informações) e visualize os recursos e as informações adicionais no painel à direita.

Escolha Pergunte a um especialista para acessar a comunidade 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 você escolher A pergunta não se aplica a essa carga de trabalho ou Nenhuma delas, AWS recomenda que você inclua o motivo na caixa Anotações. 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 AWS WA Tool console e escolha Cargas de trabalho no painel de navegação esquerdo.

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.

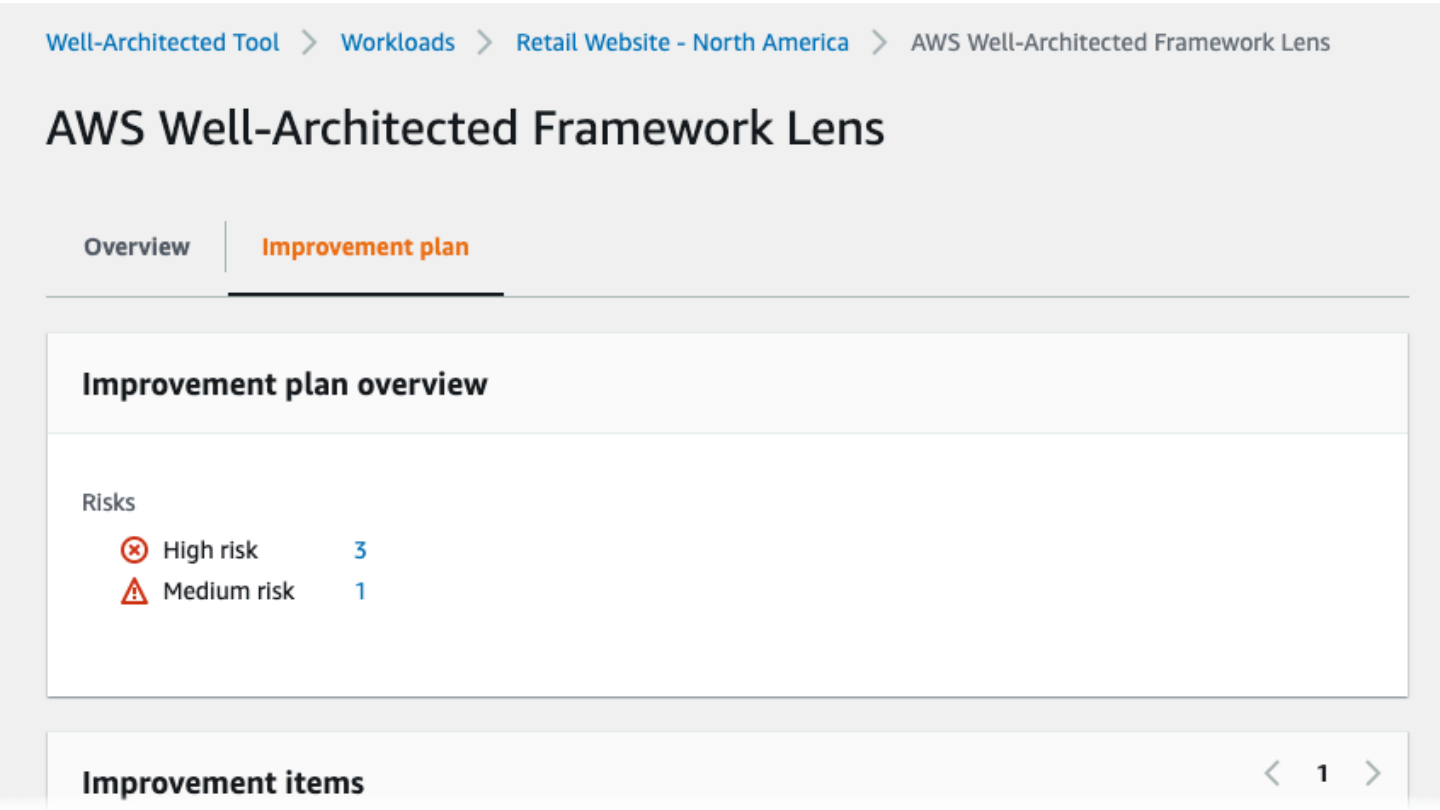
Etapa 3: Revisar o plano de aprimoramento

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

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).

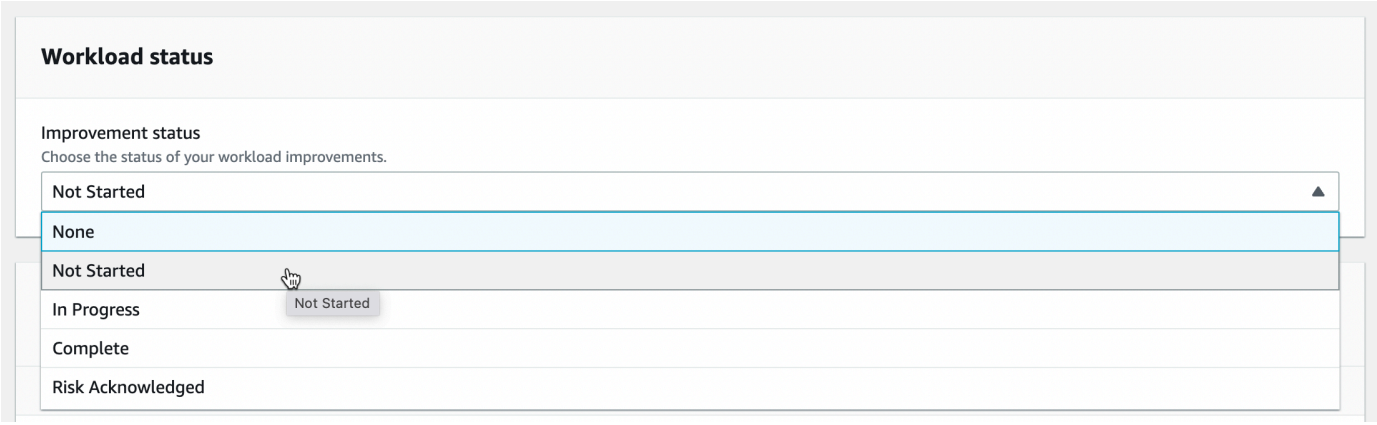
Para esse exemplo específico de carga de trabalho, três problemas de alto risco e um problema de médio risco foram identificados pelo AWS Well-Architected Framework Lens.



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.

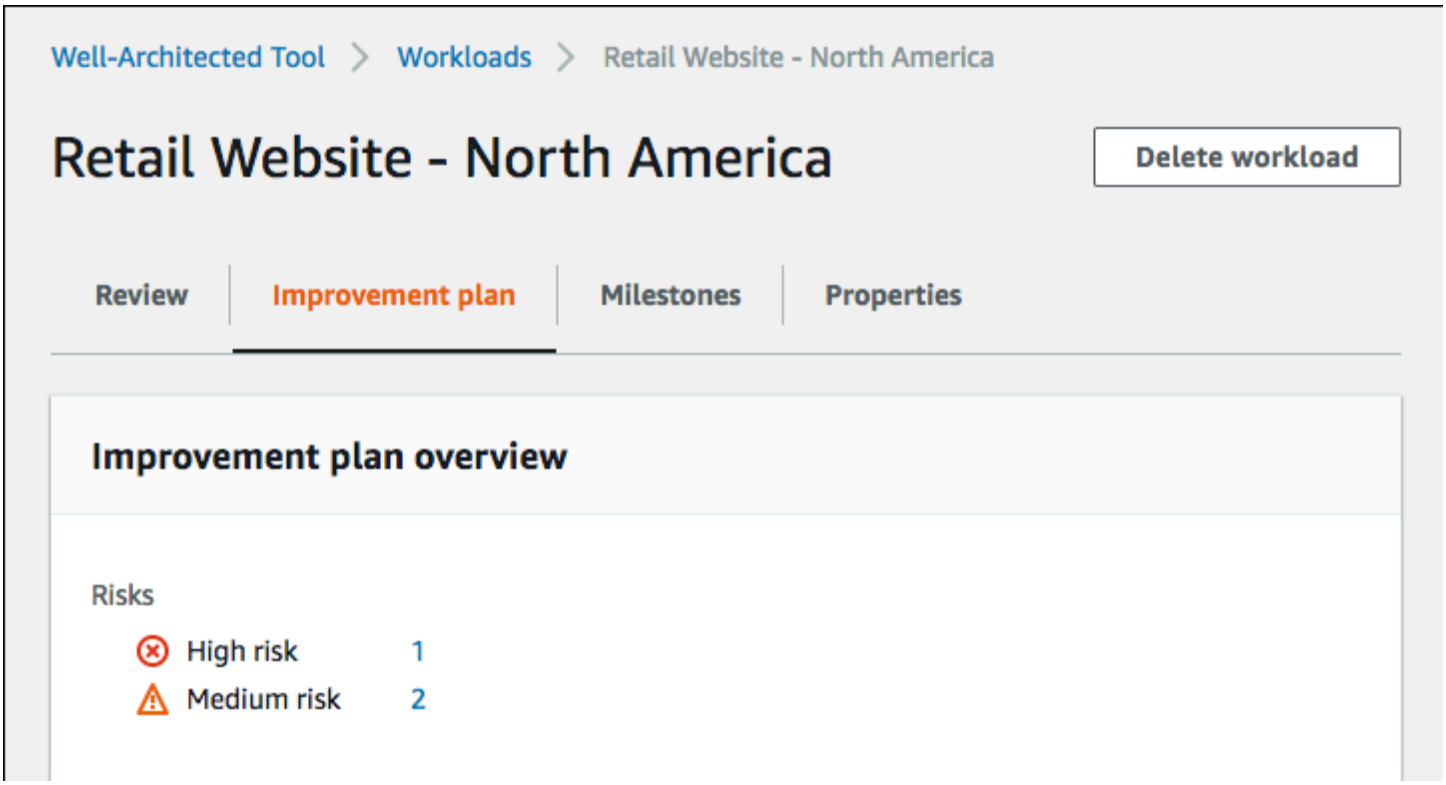
Etapa 4: Faça melhorias e avalie o progresso

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

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 carga de trabalho pode consistir em um subconjunto de recursos em um único local Conta da AWS ou ser uma coleção de vários recursos que abrangem vários locaisContas 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 possui a carga de trabalho.

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
- Completo

- Risco reconhecido

Data da 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 carga de trabalho com outros Contas da AWS usuários ou unidades organizacionais (OUs)AWS Organizations, 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 carga de trabalho 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 carga

de trabalho, o risco poderá ser menor do que o indicado. AWSsugere que os clientes documentem esses motivos e como eles afetam as melhores práticas nas notas de carga de trabalho. 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 carga de trabalho

Há duas maneiras de definir uma carga de trabalho. Na página Cargas de trabalho, AWS WA Tool você pode definir uma carga de trabalho sem um modelo. Ou, na página Modelos de revisão, você pode usar um modelo de revisão existente ou criar um novo modelo para definir uma carga de trabalho.

Para definir uma carga de trabalho na página Cargas de trabalho

1. Selecione Cargas de trabalho 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 revisão e deseja definir uma carga de trabalho a partir dele, escolha Definir a partir do modelo de revisão.
4. Siga as instruções em the section called “Definir uma workload” para especificar as propriedades da carga de trabalho ou (opcionalmente) aplicar perfis e lentes.

Para definir uma carga de trabalho na página Revisar modelos

1. Selecione Modelos de avaliação no painel de navegação esquerdo.
2. Selecione o nome de um modelo de revisão existente ou siga as instruções the section called “Criar um novo modelo do ” para criar um novo modelo de revisão.
3. Escolha Definir carga de trabalho a partir do modelo.
4. Siga as instruções em the section called “Definindo uma carga de trabalho a partir de um modelo” para criar a carga de trabalho a partir do seu modelo de revisão.

Visualizar uma carga de trabalho

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 Billing em https://console.aws.amazon.com/billing/.
2. No painel de navegação à esquerda, selecione Workloads (Cargas de trabalho).
3. Selecione a carga de trabalho a ser visualizada de uma das seguintes maneiras:
   - Selecione o nome da carga de trabalho.
   - Selecione a carga de trabalho e a opção View details (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 carga de trabalho

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 Billing em https://console.aws.amazon.com/billing/.
2. No painel de navegação à esquerda, selecione Workloads (Cargas de trabalho).
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.

   > **Note**
   >
   > Ao atualizar uma carga de trabalho existente, você pode ativarTrusted Advisor, o que cria automaticamente a função do IAM para o proprietário da carga de trabalho. Os proprietários de contas associadas para cargas de trabalho com a Trusted Advisor ativado precisam criar uma função no IAM. Para obter mais 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 carga de trabalho

Você pode compartilhar uma carga de trabalho que você possui com outros usuáriosContas da AWS, uma organização e unidades organizacionais (OUs) na mesmaRegião da AWS.

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

Para compartilhar uma carga de trabalho com outros Contas da AWS usuários

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

   Somente leitura

   Fornece acesso somente leitura à carga de trabalho.

   Colaborador

   Fornece acesso de atualização a respostas e observações, e acesso somente leitura ao restante da carga de trabalho.
7. Escolha Criar para enviar um convite de carga de trabalho 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 carga de trabalho, o convite de carga de trabalho com a permissão de nível mais alto será aplicado ao usuário.

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

Para compartilhar uma carga de trabalho com sua organização ou UOs

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool Billing em https://console.aws.amazon.com/billing/.
2. No painel de navegação à esquerda, selecione Workloads (Cargas de trabalho).
3. Selecione uma carga de trabalho que possui usando uma das seguintes formas:
   - Selecione o nome da carga de trabalho.
   - Selecione a carga de trabalho e a opção View details (Visualizar detalhes).
4. Escolha Shares (Compartilhamentos). Em seguida, escolha Criar e Criar compartilhamentos para organizações.
5. Na página Criar compartilhamento de carga de trabalho, 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 carga de trabalho.

   Colaborador

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

Para ver quem compartilhou acesso a uma carga de trabalho, escolha Shares (Compartilhamentos) na página Detalhes da carga de trabalho.

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

Você também pode compartilhar lentes personalizadas que você possui com outros usuáriosContas da AWS, sua organização e OUs na mesmaRegião da AWS. Para obter detalhes, consulte Compartilhando uma lente personalizada.

Considerações sobre compartilhamento

Uma carga de trabalho pode ser compartilhada com até 20 contas da AWS e usuários do IAM diferentes. Uma carga de trabalho só pode ser compartilhada com contas e usuários que estejam na mesma Região da AWS que a carga de trabalho.

Para compartilhar uma carga de trabalho em uma região introduzida após 20 de março de 2019, você e a Conta da AWS compartilhada devem ativar a região no AWS Management Console. Para obter mais informações, consulte Infraestrutura global da AWS.

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

Se tanto uma Conta da AWS quanto um usuário na conta tiverem convites de carga de trabalho, o convite de carga de trabalho com as permissões de nível mais alto determinará a permissão do usuário para a carga de trabalho. Se você excluir o convite de carga de trabalho para o usuário, o acesso do usuário será determinado pelo convite de carga de trabalho 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 carga de trabalho com uma organização ou uma ou mais unidades organizacionais (OUs), você deve ativar o acesso AWS Organizations.

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

Para habilitar o AWS Organizations compartilhamento

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

Excluir acesso compartilhado

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 Billing em https://console.aws.amazon.com/billing/.
2. No painel de navegação à esquerda, selecione Workloads (Cargas de trabalho).
3. Selecione a carga de trabalho usando uma das seguintes formas:
   - Selecione o nome da carga de trabalho.
   - Selecione a carga de trabalho e a opção View details (Visualizar detalhes).
4. Escolha Shares (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 carga de trabalho, será necessário excluir os dois convites de carga de trabalho para remover a permissão do usuário para a carga de trabalho.

Modificação do acesso compartilhado

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 Billing em https://console.aws.amazon.com/billing/.
2. No painel de navegação à esquerda, selecione Workloads (Cargas de trabalho).
3. Selecione uma carga de trabalho que possui usando uma das seguintes formas:
   - Selecione o nome da carga de trabalho.
   - Selecione a carga de trabalho e a opção View details (Visualizar detalhes).
4. Escolha Shares (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 carga de trabalho.

   Colaborador

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

7. Escolha Save (Salvar).

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

Aceitar e rejeitar convites de carga de trabalho

Um convite de carga de trabalho é uma solicitação para compartilhar uma carga de trabalho 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 cargas de trabalho 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 Billing em https://console.aws.amazon.com/billing/.
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 Detalhes da carga de trabalho da carga de trabalho.

Excluir uma carga de trabalho

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 carga de trabalho poderá excluí-la.

> **Warning**
>
> A exclusão de uma carga de trabalho 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 Billing em https://console.aws.amazon.com/billing/.
2. No painel de navegação à esquerda, selecione Workloads (Cargas de trabalho).
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 da carga de trabalho

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 sua carga de trabalho tiver um perfil associado, as informações gerais do perfil e os riscos priorizados serão exibidos no relatório de carga de trabalho.

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 Billing em https://console.aws.amazon.com/billing/.
2. No painel de navegação à esquerda, selecione Workloads (Cargas de trabalho).
3. Selecione a carga de trabalho desejada e escolha View details (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.

Detalhes da carga de trabalho

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 carga de trabalho poderá excluí-la.

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

Tópicos

- Guia de marcos
- Guia de propriedades
- Guia Compartilhamentos

Guia visão geral

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 de marcos

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 de propriedades

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.

Guia Compartilhamentos

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 Conta da AWS e usuário que tem acesso compartilhado à carga de trabalho:

Entidade principal

O ID da Conta da AWS ou o ARN do usuário com acesso compartilhado à carga de trabalho.

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 à conta ou ao usuário 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 da permissão

Descrição detalhada da permissão

Para compartilhar a carga de trabalho com outra conta ou usuário da Conta da AWS na mesma Região da AWS, selecione Criar. Uma carga de trabalho pode ser compartilhada com até 20 contas da AWS e usuários do IAM 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).

Lentes

As perspectivas oferecem uma maneira de você medir de forma consistente suas arquiteturas em relação às melhores práticas e identificar áreas para 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 AWS oficial. 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.

Adição de uma lente a uma workload

Para adicionar uma perspectiva a uma carga de trabalho

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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 AWS lentes, visite 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 AWS usuário ou conta, você reconhece que lentes personalizadas criadas por outros usuários e compartilhadas com você são Conteúdo de Terceiros, conforme definido no Contrato do AWS Cliente.

Remoção de uma lente de uma workload

Para remover uma perspectiva de uma carga de trabalho

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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.

   O AWS Well-Architected Framework Lens não pode ser removido de uma carga de trabalho.

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

Detalhes da lente

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

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

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 AWS Well-Architected Tool console 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 Detalhes da lente será exibida.

A página Lentes personalizadas tem os seguintes campos:

Nome

O nome da lente.

Proprietário

O Conta da AWS ID 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.

Version (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 criar uma lente personalizada

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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. 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 de AWS WA Tool validar seu arquivo JSON, sua lente personalizada é 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.

Prévia de uma lente personalizada

Para visualizar uma lente personalizada

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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 pela primeira vez

Para publicar uma lente personalizada

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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

Para publicar uma atualização em uma lente personalizada existente

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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 de AWS WA Tool validar seu arquivo JSON, sua lente personalizada é exibida em Lentes personalizadas no status DRAFT.
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.

Compartilhando uma lente personalizada

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

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

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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 Detalhes da lente, selecione Compartilhamentos. Em seguida, escolha Criar e Criar compartilhamentos com usuários ou contas para criar um convite de compartilhamento de lentes.
5. Insira o Conta da AWS ID 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 lentes para o usuário Conta da AWS ou usuário especificado.

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

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 AWS Well-Architected Tool console 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 Detalhes da lente, 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 Detalhes da lente.

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

Adição de tags a uma lente personalizada

Para adicionar tags a uma lente personalizada

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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 Save (Salvar).

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

Excluir uma lente personalizada

Para excluir uma lente personalizada

1. Faça login no AWS Management Console e abra o AWS Well-Architected Tool console 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 pessoas Contas da AWS, você reconhece que AWS disponibilizará suas lentes personalizadas para essas outras contas. Essas outras contas podem continuar acessando e usando suas lentes personalizadas compartilhadas, mesmo que você exclua as lentes personalizadas de sua conta Conta da AWS ou encerre as suas Conta da AWS.

Especificação do formato da lente

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 carga de trabalho personalizada do lens 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 carga de trabalho de 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

O AWS Well-Architected Framework Lens e outras lentes fornecidas AWS pela são atualizadas à medida que novos serviços são introduzidos, as melhores práticas existentes para sistemas baseados em nuvem são refinadas e novas práticas recomendadas são adicionadas. Quando uma nova versão de uma lente é disponibilizada, ela AWS WA Tool é atualizada 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.

Selecionar um upgrade de lente

A página Notificações exibe informações de cada workload que não está usando a versão mais atual da lente.

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

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).

Fazer upgrade de uma lente

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

> **Note**
>
> Não é possível desfazer um upgrade 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 da lente.

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

O Catálogo de Lentes é uma coleção de lentes oficiais AWS criadas AWS WA Tool que oferecem as melhores práticas focadas na up-to-date tecnologia e 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 AWS oficiais atualmente disponíveis no Catálogo de Lentes.

Nome	Descrição
AWS Estrutura Well-Architected	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	Melhores práticas para integrar a tecnologi a aos sistemas de transporte e aprimorar a experiência geral de mobilidade.
Construção de contêiner	Fornecem práticas recomendadas sobre o processo de design e criação de contêineres.
Análise de dados	Contém insights coletados de estudos de caso reais e ajuda você a aprender os principais elementos de design das cargas de trabalho de análise da Well-Architected, além de recomendações para melhorias. AWS
DevOps	Descreve uma abordagem estruturada que organizações de todos os tamanhos podem seguir para cultivar uma cultura de alta velocidade e focada na segurança, capaz de agregar valor comercial substancial usando tecnologias modernas e melhores práticas. DevOps
Governo	Melhores práticas para projetar e fornecer serviços governamentais em AWS.
Setor de saúde	Práticas recomendadas e orientações sobre como projetar, implantar e gerenciar workloads do setor de saúde na Nuvem AWS.

Nome	Descrição
IoT	Melhores práticas para gerenciar suas cargas de trabalho da Internet das Coisas (IoT) em. AWS
Criação de valor em fusões e aquisições	Fornecem um conjunto de questões adicionais a serem consideradas ao procurar maneiras de promover o crescimento da empresa, como para atividades de fusões e aquisições de capital privado.
Machine Learning	Melhores práticas para gerenciar seus recursos e cargas de trabalho de Machine Learning em AWS.
Migração	Melhores práticas de como migrar para o. Nuvem AWS
SaaS	Destinadas a projetar, implantar e arquitetar workloads de software como serviço (SaaS) na Nuvem AWS.
SAP	Princípios de design e melhores práticas para cargas de trabalho SAP no Nuvem AWS.
Aplicativos sem servidor	Práticas recomendadas para criar cargas de trabalho sem servidor. AWS Abrange cenários como microsserviços RESTful, back-ends de aplicativos móveis, processamento de fluxos e aplicações web.

Revisar os modelos do

Você pode criar modelos de avaliação no AWS WA Tool que contenham respostas pré-preenchidas para perguntas de práticas recomendadas da 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 cargas de trabalho ao realizar uma revisão do Well-Architected e ajudam a promover a consistência e a padronização das práticas recomendadas entre equipes e cargas de trabalho.

Você pode criar um modelo de avaliação para responder a perguntas comuns de melhores práticas 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 carga de trabalho a partir de um modelo de revisão, o que ajuda a escalar as melhores práticas comuns e reduzir a redundância em suas cargas de trabalho.

Criar um novo modelo do

Criar um modelo de avaliação

1. No painel de navegação, selecione Modelos de execução.
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 revisão. Todas as notas adicionadas são aplicadas a todas as cargas de trabalho que usam o modelo de revisão, enquanto as tags são específicas do modelo de revisão.

   Para obter mais informações sobre tags, consulte Marcar recursos do AWS WA Tool.
5. Escolha Next (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 revisão 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 revisão for criado, você poderá definir uma nova carga de trabalho a partir dele.

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.

Criar um novo modelo do

Para editar um modelo de avaliação

1. No painel de navegação, selecione Modelos de execução.
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 nas notas de Nome, Descrição ou Notas do modelo .
   b. Escolha Salvar modelo para atualizar o modelo de revisão com suas alterações.

4. Para atualizar quais lentes são aplicadas ao modelo de revisão, 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.

Criar um novo modelo do

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. No painel de navegação, selecione Modelos de execução.
2. Selecione o nome do modelo de avaliação que deseja compartilhar.
3. Escolha a guia Compartilhamento.
4. Para compartilhar com um usuário ou conta, escolha Criar e selecione Compartilhar com usuários ou contas 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 para 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 uma lente personalizada com uma organização ou unidades organizacionais (OUs), você deve habilitar o acessoAWS Organizations.

Definindo uma carga de trabalho a partir de um modelo

Você pode definir uma carga de trabalho a partir de um modelo de revisão que você criou ou de um modelo de revisão que foi compartilhado com você. Você não pode definir uma nova carga de trabalho a partir de um modelo de revisão que foi excluído e, se o modelo de revisão contiver uma versão desatualizada de uma lente, você deverá atualizar o modelo de revisão antes de poder definir uma nova carga de trabalho a partir dele. Para obter informações sobre como atualizar um modelo de revisão, consulte the section called “Fazer upgrade de uma lente”.

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

Para definir uma carga de trabalho a partir de um modelo de revisão

1. No painel de navegação, selecione Modelos de execução.
2. Selecione o nome do modelo de revisão a partir do qual você deseja definir uma carga de trabalho.
3. Escolha Definir carga de trabalho a partir do modelo.

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

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

   Os perfis e modelos de avaliação do Well-Architected podem ser usados em conjunto. As perguntas pré-preenchidas em seu modelo de revisão permanecem respondidas na carga de trabalho, 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).

Criar um novo modelo do

Para excluir um modelo de revisão

1. No painel de navegação, selecione Modelos de execução.
2. Na seção Modelos de avaliação, escolha o modelo de revisão 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 revisão.

3. Na caixa de diálogo Excluir modelo de revisão, insira o nome do modelo de revisão no campo para confirmar a exclusão.
4. Escolha Delete (Excluir).

Não é possível criar uma nova carga de trabalho a partir de um modelo de revisão que tenha sido excluído. Se você compartilhou um modelo de revisão excluído com outros usuários, contas ou organizações do IAM, eles não poderão criar cargas de trabalho a partir dele.

Perfis

Você pode criar perfis para fornecer seu contexto comercial e identificar metas que gostaria de alcançar ao realizar uma revisão do Well-Architected. AWS Well-Architected Toolusa 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 carga de trabalho. Anexar um perfil à sua carga de trabalho 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 carga de trabalho ou adicionar um perfil a uma carga de trabalho existente.

Criar um perfil do

Como criar um perfil

1. No painel de navegação, selecione Roles (Funções).
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 carga de trabalho 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 carga de trabalho.

   Para obter mais informações sobre tags, consulte Marcar recursos do AWS WA Tool.
6. Escolha Save (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.

Editação de um perfil

Como editar um perfil

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

Editação de um perfil

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. No painel de navegação, selecione Roles (Funções).
2. Selecione o nome do perfil que deseja compartilhar.
3. Escolha a guia Compartilhamento.
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 Create e selecione Create shares to Organizations. Para compartilhar com uma organização inteira, selecione Conceder permissões para 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 uma lente personalizada com uma organização ou unidades organizacionais (OUs), você deve habilitar o AWS Organizations acesso.

Adicionar um perfil a uma carga de trabalho

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

Para obter mais informações sobre como adicionar um perfil ao definir uma carga de trabalho, consultethe section called “Definir uma workload”.

Para adicionar um perfil a uma carga de trabalho existente

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

   > **Note**
   >
   > Somente um perfil pode ser associado a uma carga de trabalho.

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

A visão geral da carga de trabalho exibe uma contagem de perguntas priorizadas respondidas e riscos priorizados com base nas informações do perfil associado. Escolha Continuar revisando para abordar as questões priorizadas na revisão da carga de trabalho. Para obter 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 carga de trabalho.

Para remover uma perspectiva de uma carga de trabalho

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

Para remover um perfil de uma carga de trabalho

1. Na seção Perfis da carga de trabalho, escolha Remover.
2. Para confirmar a remoção, insira o nome do perfil no campo de entrada de texto.
3. Escolha Remove.

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

Excluir um perfil do AWS WA Tool

Se você criou um perfil, poderá excluí-lo da lista de perfis disponíveis emAWS WA Tool.

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

Para remover um perfil da sua lista de perfis

1. No painel de navegação, selecione Roles (Funções).
2. Selecione o nome do perfil que você deseja remover.
3. Escolha Delete (Excluir).
4. Para confirmar a remoção, digite o nome do perfil no campo de entrada de texto.
5. Escolha Delete (Excluir).

Se você quiser manter um perfil na sua lista de perfis, mas removê-lo de uma carga de trabalho, consultethe section called “Para remover uma perspectiva de uma carga de trabalho”.

AWS Well-Architected Tool Conector para Jira

Você pode usar o AWS Well-Architected Tool Connector for Jira para vincular sua conta do Jira AWS Well-Architected Tool e sincronizar itens de melhoria de suas cargas de trabalho com projetos do Jira para ajudá-lo a criar um mecanismo de ciclo fechado na implementação de melhorias.

O conector fornece sincronização automática e manual. Para obter mais detalhes, consulte Configurando o conector.

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

Você pode optar por sincronizar os itens de melhoria com o projeto padrão do WA Jira ou especificar uma chave de projeto existente para sincronizar. No nível da carga de trabalho, você pode sincronizar cada carga de trabalho 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: Carga de trabalho
- Tarefa: Pergunta
- Subtarefa: Melhores práticas
- Rótulo: Pillar

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.

Configurando o conector

Para 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 Aplicativos e, em seguida, selecione Explorar mais aplicativos.
3. Na página Descubra aplicativos e integrações para o Jira, insira AWS Well-Architected. Em seguida, escolha o AWS Well-Architected Tool Conector para Jira.
4. Na página do aplicativo, escolha Obter aplicativo.
5. No painel Adicionar ao Jira, escolha Obter agora.
6. Após a instalação do aplicativo, para concluir a configuração, escolha Configurar.
7. Na página AWS Well-Architected Tool Configuração, escolha Connect a new Conta da AWS.
8. Digite seu AccessKeyID e chave secreta. Opcional: insira seu token de sessão. Em seguida, escolha Connect.

   > **Note**
   >
   > Certifique-se de que sua conta tenha a permissão`wellarchitected:ConfigureIntegration`. Essas permissões são necessárias para adicionar Contas da AWS ao Jira.
   > Vários Contas da AWS podem ser conectados AWS WA Tool.

   > **Note**
   >
   > Como prática recomendada de segurança, é altamente recomendável usar credenciais de IAM de curto prazo. Para obter detalhes sobre como criar uma AccessKeyID e uma chave secreta para você Conta da AWS, consulte Gerenciamento de chaves de acesso

(console) e, para obter detalhes sobre o uso de credenciais de curto prazo, consulte Solicitação de credenciais temporárias.

9. Em Regiões, selecione a que Regiões da AWS você deseja conectar. Em seguida, escolha Connect.

Configuração do projeto Jira

Ao usar projetos personalizados, verifique se você tem os seguintes tipos de problemas na configuração do seu projeto:

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

Para obter detalhes sobre como gerenciar tipos de problemas, consulte Atlassian Support | Adicionar, editar e excluir um tipo de problema.

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

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

O conector agora está configurado e pronto para ser configurado. Para definir as configurações de sincronização do Jira no nível da conta e da carga de trabalho, consulte Configuração do conector.

Configurar o conector do

Com o AWS Well-Architected Tool Connector for Jira, você pode configurar a sincronização do Jira no nível da conta, no nível da carga de trabalho ou em ambos. Você pode definir as configurações do Jira no nível da carga de trabalho, independentemente das configurações no nível da conta, ou substituir as configurações no nível da conta em uma carga de trabalho específica para especificar o comportamento de sincronização da carga de trabalho. Você também pode definir as configurações do Jira ao definir uma carga de trabalho.

O conector fornece dois métodos de sincronização: sincronização automática e manual. Em ambos os métodos de sincronização, as alterações feitas no Jira 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 em AWS WA Tool modificar sua carga de trabalho em resposta às mudanças no Jira.
> Se você tiver informações confidenciais que não deseja sincronizar com o Jira, não insira essas informações no campo Notas em suas cargas de trabalho.

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

Para configurar o conector no nível da conta

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

> **Note**
>
> A chave de projeto especificada do Jira é usada para todas as cargas de trabalho, a menos que você altere o projeto no nível da carga de trabalho.

5. Escolha Salvar configurações.

Para configurar o conector no nível da carga de trabalho

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

> **Note**
>
> As configurações do nível da conta de substituição devem ser selecionadas para aplicar as configurações específicas da carga de trabalho.

5. Em Substituição de sincronização, selecione uma das seguintes opções:
   a. Para excluir a carga de trabalho da sincronização do Jira, selecione Não sincronizar carga de trabalho.
   b. Para escolher manualmente quando sincronizar a carga de trabalho, selecione Sincronizar carga de trabalho - Manual.
   c. Para sincronizar as alterações da carga de trabalho automaticamente, selecione Sincronizar carga de trabalho - Automático.
6. (Opcional) Para a chave do projeto do Jira, insira a chave do projeto com a qual sincronizar a carga de trabalho. 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 cria um projeto WA Jira.
7. Escolha Salvar.

Para obter detalhes sobre como realizar uma sincronização manual, consulte Sincronização de uma carga de trabalho.

Sincronizando uma carga de trabalho

Para sincronização automática, o conector sincroniza automaticamente os itens de melhoria quando você atualiza uma carga de trabalho (por exemplo, ao preencher uma pergunta ou selecionar uma nova prática recomendada).

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

Para sincronizar manualmente uma carga de trabalho

1. Quando você estiver pronto para sincronizar sua carga de trabalho com o Jira, selecione Cargas de trabalho no painel de navegação esquerdo. Em seguida, selecione a carga de trabalho que você deseja sincronizar.
2. Na visão geral da carga de trabalho, escolha Sincronizar com o Jira.
3. Selecione a lente que você deseja sincronizar.
4. Para que as perguntas sejam sincronizadas com o Jira, selecione as perguntas ou os pilares inteiros que você deseja sincronizar com o projeto Jira.
    - Para qualquer pergunta que você queira remover, selecione o ícone X ao lado do título da pergunta.
5. Escolha Sincronizar.

Desinstalando o conector

Para desinstalar completamente o AWS Well-Architected Tool Connector for Jira, execute as seguintes tarefas:

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

Para desativar o conector no nível da conta

> **Note**
>
> As etapas a seguir são executadas em seu Conta da AWS.

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

Para desvincular um 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 Aplicativos e, em seguida, selecione Gerenciar seus aplicativos.
3. Escolha a seta suspensa ao lado de AWS Well-Architected Tool Connector for Jira e, em seguida, escolha Configurar.
4. No painel AWS Well-Architected Tool Configuração, para desvincular um Conta da AWS, escolha X em Ações.

Para desinstalar o conector

> **Note**
>
> Todas as etapas a seguir são executadas na sua conta do Jira, não na sua Conta da AWS. Recomendamos verificar se todos os conectados Contas da AWS estão desvinculados na configuração do conector antes de desinstalar o conector.

1. Faça login na sua conta do Jira.
2. Na barra de navegação superior, escolha Aplicativos e, em seguida, selecione Gerenciar seus aplicativos.
3. Escolha a seta suspensa ao lado de AWS Well-Architected Tool Connector for Jira.
4. Escolha Desinstalar e, em seguida, escolha Desinstalar aplicativo.

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.

Compartilhe convites

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

- Se você aceitar um convite de carga de trabalho, a carga de trabalho será adicionada às suas páginas de Cargas de trabalho e Painel de controle.
- 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 revisão, o modelo será adicionado à sua página de modelos de revisão.

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

> **Note**
>
> Cargas de trabalho, lentes personalizadas, perfis e modelos de revisão só podem ser compartilhados na mesma região Região da AWS.

O proprietário da carga de trabalho controla quem tem acesso compartilhado.

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

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

Nome

O nome da carga de trabalho, da lente personalizada ou do modelo de revisão a ser compartilhado.

Tipo de recurso

O tipo de convite: Carga de trabalho, Lente personalizada, Perfis ou Modelo de revisão.

Proprietário

O ID da Conta da AWS que possui a carga de trabalho.

Permissão

A permissão que você receberá para a carga de trabalho.

- Somente leitura

  Fornece acesso somente de leitura à carga de trabalho, às lentes personalizadas, aos perfis ou ao modelo de revisão.

- Colaborador

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

Detalhes da permissão

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 carga de trabalho, a carga de trabalho é adicionada às páginas Cargas de trabalho e Painel de controle. 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 revisão, o modelo é adicionado à página Modelos de revisão.

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 carga de trabalho, o convite de carga de trabalho para o usuário determinará a permissão do usuário.

Rejeitar um convite de compartilhamento

Para rejeitar um convite de compartilhamento

1. Selecione a carga de trabalho 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 cargas de trabalho e modelos de revisão que têm lentes e perfis associados a eles. É possível atualizar para a versão mais recente de uma lente ou perfil para uma carga de trabalho 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 revisão para notificá-lo. Se você visualizar uma carga de trabalho específica ou um modelo de revisão 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 cargas de trabalho 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 carga de trabalho ou um modelo de revisão.

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

Notificações de perfil

Há dois tipos de notificações de perfil:

- Atualização do perfil
- Exclusão de perfil

Quando um perfil associado a uma carga de trabalho tiver sido editado (para obter mais informações, consulte the section called “Editação 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 carga de trabalho associada ao perfil excluído, receberá uma notificação de que ainda poderá usar o perfil na carga de trabalho existente, mas não poderá adicioná-lo a novas cargas de trabalho.

Para atualizar uma versão de perfil

1. No painel de navegação à esquerda, selecione Notificações.
2. Selecione o nome da carga de trabalho na lista da guia Notificações de perfil ou use a barra de pesquisa para pesquisar pelo nome da carga de trabalho.
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.

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

Consulte Perfis para obter mais informações.

Painel

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

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

Resumo

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

Escolha Incluir cargas de trabalho compartilhadas comigo para que as estatísticas resumidas, o relatório consolidado e as outras seções do painel reflitam tanto as suas cargas de trabalho quanto as cargas de trabalho 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

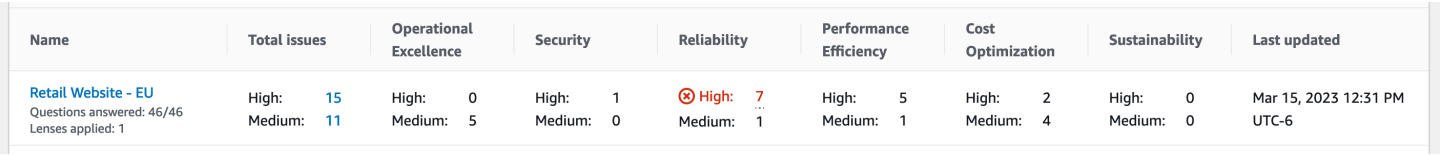
A seção Problemas da Well-Architected Framework por pilar mostra uma representação gráfica do número de problemas de alto e médio risco por pilar para todas as cargas de trabalho.

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

> **Note**
>
> Somente edições da lente Well-Architected Framework estão incluídas nesta seção.

Problemas do Well-Architected Framework por pilar

A seção Problemas da Well-Architected Framework por carga de trabalho exibe informações para cada carga de trabalho.



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 carga de trabalho também são mostrados.

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

Total de problemas

O número total de problemas identificados pela lente Well-Architected Framework para a carga de trabalho.

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 carga de trabalho 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.

Data da última atualização

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

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

> **Note**
>
> Somente edições da lente Well-Architected Framework estão incluídas nesta seção.

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

A seção Problemas Well-Architected Framework por item do plano de melhoria exibe os itens do plano de melhoria para todas as suas cargas de trabalho. 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.

Cargas de trabalho aplicáveis

O número de cargas de trabalho às quais esse plano de aprimoramento se aplica.

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

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

Segurança em AWS Well-Architected Tool

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade aplicáveis AWS Well-Architected Tool, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço 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 você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS WA Tool. Os tópicos a seguir mostram como configurar para atender AWS WA Tool aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS WA Tool recursos.

Tópicos

Proteção de dados em AWS Well-Architected Tool

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Well-Architected Tool. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu 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 Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS LGPD e Modelo de Responsabilidade Compartilhada no AWS Blog de Segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários 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. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão 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 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS WA Tool ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou 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, recomendemos 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 lá AWS WA Tool são criptografados em trânsito.

Como AWS usa seus dados

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

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

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

A equipe do AWS Well-Architected não tem acesso a:

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

Gerenciamento de identidade e acesso para AWS Well-Architected Tool

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS WA Tool os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS WA Tool.

Usuário do serviço — Se você usar o AWS WA Tool serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS WA Tool recursos para fazer seu trabalho, talvez precise 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 atributo no AWS WA Tool, consulte Solução de problemas AWS Well-Architected Tool de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS WA Tool recursos da sua empresa, provavelmente tem acesso total AWS WA Tool a. É seu trabalho determinar quais AWS WA Tool recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua

empresa pode usar o IAM com AWS WA Tool, consulteComo 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 acesso ao AWS WA Tool. Para ver exemplos de políticas AWS WA Tool baseadas em identidade que você pode usar no IAM, consulte. AWS Well-Architected Tool exemplos de políticas baseadas em identidade

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e 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. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Utilizar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou 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 usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. 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 AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos 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, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne 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 Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

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

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode 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 pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você 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 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, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos 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 aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar 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.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você 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.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. 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.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada 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 políticas AWS JSON 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 funções não têm permissões. Para conceder aos usuários permissões 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 presumir os perfis.

As políticas do IAM definem permissões para uma ação independente 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 função da AWS Management Console AWS CLI, da ou da AWS API.

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 do IAM, grupo de usuários ou perfil. 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 Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente 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 autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF 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

AWS oferece suporte a tipos de políticas adicionais 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 atributo 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 (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) 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 atributo. 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 AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS Well-Architected Tool funciona com o IAM

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

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

Atributo do IAM	AWS WA Tool apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim

Atributo do IAM	AWS WA Tool apoio
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 ter uma visão de alto nível de como AWS WA Tool e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade do AWS WA Tool

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API 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 dentro AWS WA Tool

Oferece 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, 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 atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) 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. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para AWS WA Tool

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de

AWS API 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 políticas 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 de AWS WA Tool ações, consulte Ações definidas por AWS Well-Architected Tool na Referência de autorização de serviço.

recursos de políticas

Oferece compatibilidade com recursos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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 AWS WA Tool recursos e seus ARNs, consulte Recursos definidos por AWS Well-Architected Tool na Referência de Autorização de Serviço. Para saber com quais

ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Well-Architected Tool.

O recurso AWS WA Tool de carga de trabalho tem o seguinte ARN:

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

Para obter mais informações sobre o formato dos ARNs, consulte Amazon Resource Names (ARNs) e AWS Service Namespaces.

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 AWS WA Tool ações, como aquelas para criar e listar cargas de trabalho, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

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

Para ver uma lista dos tipos de AWS WA Tool recursos e seus ARNs, consulte Recursos definidos por AWS Well-Architected Tool na Referência de autorização de 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 política para AWS WA Tool

Suporta chaves de condição de política específicas de serviço	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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 `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. 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 atributo 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.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

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

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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 `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. 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 atributo 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.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

ACLs em AWS WA Tool

Oferece compatibilidade 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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Autorização baseada em tags do AWS WA Tool

Oferece compatibilidade com ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação 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 onde 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 oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS WA Tool

Oferece compatibilidade com credenciais temporárias	Sim

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

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. 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 (console) no Guia do usuário do IAM.

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

Permissões principais entre serviços para AWS WA Tool

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um

serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para AWS WA Tool

Oferece suporte a perfis de serviço	Não

Um perfil de serviço é um perfil do IAM que um serviço assume para realizar 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 a serviços para AWS WA Tool

Oferece suporte a perfis vinculados ao serviço	Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados 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 Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

AWS Well-Architected Tool exemplos de políticas baseadas em identidade

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS WA Tool . Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. 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

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS WA Tool recursos 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 AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam 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 atributos 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 gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como 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 100 verificações de política e recomendações acionáveis para ajudá-lo 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 você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS 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 AWS Well-Architected Tool console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS WA Tool recursos em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do 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 AWS WA Tool console, anexe também a seguinte política AWS gerenciada 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.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. 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 programaticamente usando a API AWS CLI ou 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 acesso Conta da AWS total às suas cargas de trabalho. O acesso total permite que o usuário execute todas as ações em 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 Conta da AWS somente de leitura às suas cargas de trabalho. 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 sua conta acesso Conta da AWS somente de leitura a uma de suas cargas de trabalho,99999999999955555555555566666666, na região. `us-west-2` 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/99999999999955555555555666666666"
     }
   ]
}
```

Usando uma chave de condição específica do serviço para o AWS Well-Architected Tool Connector for Jira

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

A seguir, descrevemos os usos relevantes da chave de condição:

- **`CreateWorkload:`** Ao se inscrever `wellarchitected:JiraProjectKeyCreateWorkload`, você pode definir quais projetos personalizados do Jira podem ser vinculados a qualquer carga de trabalho criada pelo usuário. Por exemplo, se um usuário tentar criar uma nova carga de trabalho com o projeto ABC, mas a política especificar apenas o projeto PQR, a ação será negada.
- **`UpdateWorkload:`** Ao se inscrever `wellarchitected:JiraProjectKeyUpdateWorkload`, você pode definir quais projetos personalizados do Jira podem ser vinculados a essa carga de

trabalho específica ou a qualquer carga de trabalho. Por exemplo, se um usuário tentar atualizar uma carga de trabalho existente com o projeto ABC, mas a política especificar o projeto PQR, a ação será negada. Além disso, se o usuário tiver uma carga de trabalho vinculada ao projeto PQR e tentar atualizá-la para ser vinculada ao projeto ABC, a ação será negada.

- **`UpdateGlobalSettings:`**Ao se `wellarchitected:JiraProjectKey` inscrever`UpdateGlobalSettings`, você pode definir quais projetos personalizados do Jira podem ser vinculados ao Conta da AWS. A configuração no nível da conta protege as cargas de trabalho em sua conta que não substituem as configurações do Jira no nível da conta. Por exemplo, se um usuário tiver acesso a`UpdateGlobalSettings`, ele não poderá vincular cargas de trabalho 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"]
    }
   }
```

```
  }
 ]
}
```

AWS políticas gerenciadas para AWS Well-Architected Tool

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

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

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

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

AWS política gerenciada: WellArchitectedConsoleFullAccess

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

Esta política concede acesso total AWS Well-Architected Tool a.

Detalhes da permissão

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

```
   ]
}
```

AWS política gerenciada: WellArchitectedConsoleReadOnlyAccess

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

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

Detalhes da permissão

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

AWS política gerenciada: AWSWellArchitectedOrganizationsServiceRolePolicy

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

Essa política concede permissões administrativas necessárias para apoiar a AWS Well-Architected Tool integração com Organizations. AWS Organizations Essas permissões permitem que a conta de gerenciamento da organização habilite o compartilhamento de recursos com AWS WA Tool.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `organizations:ListAWSServiceAccessForOrganization`— Permite que os diretores verifiquem se o acesso ao AWS serviço está habilitado para 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": "*"
        }
    ]
}
```

AWS política gerenciada: AWSWellArchitectedDiscoveryServiceRolePolicy

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

Essa política permite AWS Well-Architected Tool acessar AWS serviços e recursos relacionados a AWS WA Tool recursos.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `trustedadvisor:DescribeChecks`— Lista as Trusted Advisor verificações disponíveis.
- `trustedadvisor:DescribeCheckItems`— Busca dados de Trusted Advisor cheques, incluindo status e recursos sinalizados por. Trusted Advisor
- `servicecatalog:GetApplication`— Busca detalhes de um AppRegistry aplicativo.
- `servicecatalog:ListAssociatedResources`—Lista os recursos associados a um AppRegistry aplicativo.
- `cloudformation:DescribeStacks`: obtém detalhes de pilhas do AWS CloudFormation .
- `cloudformation:ListStackResources`—Lista os recursos associados às AWS CloudFormation pilhas.
- `resource-groups:ListGroupResources`—Lista os recursos de um ResourceGroup.
- `tag:GetResources`— Necessário 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 um aplicativo. AppRegistry
- `servicecatalog:UpdateAttributeGroup`: atualiza um grupo de atributos gerenciado pelo serviço.
- `servicecatalog:DisassociateAttributeGroup`—Desassocia um grupo de atributos gerenciados pelo serviço de um aplicativo. 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-*"
   ]
  }
 ]
}
```

AWS WA Tool atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS WA Tool desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS WA Tool documento.

Alteração	Descrição	Data
AWS WA Tool política gerenciada alterada	`"wellarchitected:Export*"` Adicionado a `WellArchitectedConsoleReadOnlyAccess` .	22 de junho de 2023
AWS WA Tool política de função de serviço adicionada	Adicionado `AWSWellArchitectedDiscoveryServiceRolePolicy` para AWS Well-Architected Tool permitir o acesso a AWS serviços e recursos relacionados a AWS WA Tool recursos.	3 de maio de 2023
AWS WA Tool permissões adicionadas	Foi adicionada uma nova ação a `ListAWSServiceAccessForOrganization` ser concedida AWS WA Tool para permitir verificar se o acesso	22 de julho de 2022

Alteração	Descrição	Data
	ao AWS serviço está habilitado o AWS WA Tool.	
AWS WA Tool começou a rastrear as alterações	AWS WA Tool começou a rastrear as mudanças em suas políticas AWS gerenciadas.	22 de julho de 2022

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

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS WA Tool um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS WA Tool

Não estou autorizado a realizar uma ação em AWS WA Tool

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário *mateojackson* tenta usar o console para executar a ação`DeleteWorkload`, 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 em AWS Well-Architected Tool

A resposta a incidentes AWS Well-Architected Tool é uma AWS responsabilidade. AWS tem uma política e um programa formais e documentados que regem a resposta a incidentes.

AWS problemas operacionais com amplo 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 informações sobre como usar o AWS Health Dashboard, consulte o Guia AWS Health do usuário.

Validação de conformidade para AWS Well-Architected Tool

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção 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)).

- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno 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 — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS Well-Architected Tool

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. 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 zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura em AWS Well-Architected Tool

Como serviço gerenciado, AWS Well-Architected Tool é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a

infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS WA Tool pela rede. Os clientes devem oferecer suporte para:

- 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 configuração e vulnerabilidade em AWS Well-Architected Tool

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

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

O problema de "confused deputy" é uma questão de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. 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 usar as chaves de contexto de condição `aws:SourceAccount`global `aws:SourceArn`e as chaves de contexto nas políticas de recursos para limitar as permissões que AWS Well-Architected Tool concedem outro serviço ao recurso. Use `aws:SourceArn` se quiser apenas um recurso associado a acessibilidade de serviço. 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 você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto AWS WA Tool para evitar o confuso problema substituto.

```
{
  "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 seusAWS WA Tool recursos

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

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

Observações

- O compartilhamento de um recurso o torna disponível para uso por diretores 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 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 pela 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 AWS WA Tool ou AWS Command Line Interface (AWS CLI) para habilitar o compartilhamento com 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 estiver conectado como principal na conta de gerenciamento da organização.
- A organização deve ter todos os atributos habilitados. Para obter mais informações, consulte Habilitar todos os recursos na sua organização 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 Billing em https://console.aws.amazon.com/billing/.

   Você pode executar essas etapas somente enquanto estiver conectado como diretor na conta de gerenciamento da organização.

2. No painel de navegação à esquerda, escolha Settings (Configurações).
3. Escolha Ativar suporte AWS Organizations.
4. Escolha Save settings (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 Billing em https://console.aws.amazon.com/billing/.

   Você pode executar essas etapas somente enquanto estiver conectado como diretor na conta de gerenciamento da organização.
2. No painel de navegação à esquerda, escolha Settings (Configurações).
3. Desmarque Ativar suporte AWS Organizations.
4. Escolha Save settings (Salvar configurações).

Marcar recursos do AWS WA Tool

Para ajudar você a gerenciar os recursos do AWS WA Tool, é possível atribuir seus próprios metadados a cada recurso na forma de tags. Este tópico descreve as etiquetas e mostra como criá-las.

Índice

Conceitos básicos de tags

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

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

Além disso, as tags não são automaticamente atribuídas aos recursos. Depois de adicionar uma tag, você pode editar as chaves e os valores das tags ou remover tags de um recurso a qualquer momento. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

As tags não têm significado semântico no AWS WA Tool e são interpretadas estritamente como uma sequência dos caracteres. É possível definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo.

Você pode trabalhar com tags usando o AWS Management Console, a AWS CLI e a API do 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.

Marcar recursos da

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 cargas de trabalho existentes, você pode aplicar tags na guia Propriedades. Para lentes personalizadas, perfis e modelos de revisão existentes, você pode aplicar tags na guia Visão geral.

Se você estiver usando a API do AWS WA Tool, a AWS CLI ou um AWS SDK, será possível aplicar tags a novos recursos usando o parâmetro `tags` na ação da API relevante ou, para recursos existentes, usar a ação da API `TagResource`. Para obter mais informações, consulte TagResource.

Algumas ações de criação de recursos permitem que você especifique tags para um recurso quando ele é criado. Se as tags não puderem ser aplicadas durante a criação dos recursos, haverá falha no processo de criação de recursos. Isso garante que os recursos que você pretende marcar na criação sejam criados com as tags especificadas ou não sejam criados. Se você marcar recursos no momento da criação, não precisará executar scripts de marcação personalizados após a criação do recurso.

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

Suporte à marcação para recursos do AWS WA Tool

Recurso	Compatível com tags	Oferece suporte à propagação de tags	Compatível com o uso de tags na criação (API do AWS WA Tool, AWS CLI e AWS SDK)
Cargas de trabalho do AWS WA Tool	Sim	Não	Sim
AWS WA ToolLentes personalizadas	Sim	Não	Sim

Recurso	Compatível com tags	Oferece suporte à propagação de tags	Compatível com o uso de tags na criação (API do AWS WA Tool, AWS CLI e AWS SDK)
AWS WA ToolPerfis do	Sim	Não	Sim
modelos de revisão do AWS WA Tool	Sim	Não	Sim

Restrições de tags

As restrições básicas a seguir se aplicam às tags:

- Número máximo de tags por recurso: 50
- Em todos os recursos, cada chave de etiqueta deve ser exclusiva e pode ter apenas um valor.
- Comprimento máximo da chave: 128 caracteres Unicode em UTF-8
- Comprimento máximo do valor: 256 caracteres Unicode em UTF-8
- Se seu esquema de marcação for usado em vários serviços e recursos da AWS, lembre-se de que outros serviços podem ter restrições nos caracteres permitidos. Em geral, os caracteres permitidos são: letras, números, espaços representáveis em UTF-8 e os seguintes caracteres: + - = . _ : / @.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- Não use `aws:`, `AWS:` nem qualquer combinação de letras maiúsculas e minúsculas dessas strings como um prefixo para chaves ou valores, pois são reservadas para uso da AWS. Você não pode editar nem excluir chaves nem valores de etiquetas com esse prefixo. As tags com esse prefixo não contam nos limites de tags por recurso.

Trabalhar 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.

Adicionar e excluir tags em um recurso individual

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

Para adicionar ou excluir uma tag em uma carga de trabalho

1. Faça login no AWS Management Console e abra o console do AWS Well-Architected Tool Billing em https://console.aws.amazon.com/billing/.
2. Na barra de navegação, selecione a região a ser usada.
3. No painel de navegação, selecione Cargas de trabalho.
4. Selecione a carga de trabalho a ser modificada e escolha Propriedades.
5. Na seção Tags, escolha Manage tags (Gerenciar tags).
6. Adicione ou exclua suas tags conforme necessário.
   - Para adicionar uma nova tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
   - Para excluir uma tag, escolha Remove (Remover).
7. Repita esse processo para cada tag que você deseja adicionar ou excluir. Escolha Save (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 Billing em https://console.aws.amazon.com/billing/.
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 suas tags conforme necessário.

- Para adicionar uma nova tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
- Para excluir uma tag, escolha Remove (Remover).

7. Repita esse processo para cada tag que você deseja adicionar ou excluir. Escolha Save (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 Billing em https://console.aws.amazon.com/billing/.
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 suas tags conforme necessário.

   - Para adicionar uma nova tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
   - Para excluir uma tag, escolha Remove (Remover).

7. Repita esse processo para cada tag que você deseja adicionar ou excluir. Escolha Save (Salvar) para salvar as alterações.

Para adicionar ou excluir uma tag em um modelo de revisão

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

   - Para adicionar uma nova tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.

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

7. Repita esse processo para cada tag que você deseja adicionar ou excluir. Escolha Save (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 do AWS WA Tool

Tarefa	Ação de 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 as tags ao criar o recurso. As ações a seguir são compatíveis com o uso de tags na criação.

Tarefa	Ação de API
Criar uma carga de trabalho	CreateWorkload
Importar uma nova lente	ImportLens
Como criar um perfil do	CreateProfile
Criar um modelo de revisão	CreateReviewTemplate

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

O AWS Well-Architected Tool é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no AWS WA Tool. O CloudTrail captura as chamadas de API do AWS WA Tool como eventos. As chamadas capturadas incluem as chamadas do console do AWS WA Tool e as chamadas de código para as operações da API do AWS WA Tool. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o AWS WA Tool. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o AWS WA Tool, endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

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 com outros eventos de serviços da AWS em Event history (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 em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços AWS para analisar mais ainda e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o 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:

- Se a solicitação foi feita com credenciais de usuário ou de usuário root.
- 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 obter mais informações, consulte o Elemento userIdentity do 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 do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

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

```
   {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-
west-2.amazon.com",
```

```
        "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-
test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
                "accountId": "444455556666",
                "userName": "well-architected-api-svc-integ-test-read-write"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-10-14T03:41:39Z"
            }
        }
    },
    "eventTime": "2020-10-14T04:43:13Z",
    "eventSource": "wellarchitected.amazonaws.com",
    "eventName": "CreateWorkload",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.178",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.848
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
 java/1.8.0_262 vendor/Oracle_Corporation",
    "requestParameters": {
           "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
           "Description": "***",
           "AwsRegions": [
               "us-west-2"
           ],
           "ReviewOwner": "***",
           "Environment": "PRODUCTION",
           "Name": "***",
           "Lenses": [
               "wellarchitected",
               "serverless"
           ]
    },
    "responseElements": {
```

```
        "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
        "Id": "8cdcdf7add10b181fdd3f686dacffdac"
    },
    "requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
    "eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

EventBridge

O AWS Well-Architected Tool envia eventos para o Amazon EventBridge quando ações são realizadas em recursos bem arquitetados. É possível usar o EventBridge e esses eventos para escrever regras que executam ações, como notificá-lo, 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
  - Atualizando as propriedades de uma carga de trabalho
  - Como compartilhar ou cancelar o compartilhamento de workload
  - Atualizar o status de um convite de compartilhamento
  - Adicionar ou remover tags
  - Atualizando uma resposta
  - Atualizar notas de revisão
  - Adicionar ou remover uma lente de uma carga de trabalho
- Relacionado à lente
  - Importar ou exportar uma lente personalizada
  - publicar uma lente personalizada
  - Exclusão de uma lente personalizada
  - Como compartilhar ou cancelar o compartilhamento de uma lente personalizada
  - Atualizar o status de um convite de compartilhamento
  - Adicionar ou remover uma lente de uma carga de trabalho

Exemplo de eventos do AWS WA Tool

Esta seção inclui exemplos de eventos do AWS Well-Architected Tool.

Atualizando uma resposta em uma carga de trabalho


```
{
  "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"
   }
}
```

Publicação de 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: 16 de abril de 2024

Alteração	Descrição	Data
Jira	Esta versão adicionou o AWS Well-Architected Tool Connector for 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 Lens Catalog ao AWS WA Tool.	26 de novembro de 2023
Funcionalidade atualizada	Esta versão adiciona o recurso Modelos de revisão ao AWS WA Tool.	3 de outubro de 2023
WellArchitectedConsoleReadOnlyAccess política gerenciada atualizada	`"wellarchitected:ExportLens"` Adicionado a `WellArchitectedConsoleReadOnlyAccess` .	22 de junho de 2023
Funcionalidade atualizada	Esta versão adiciona o recurso Perfis ao AWS WA Tool.	13 de junho de 2023
Funcionalidade atualizada	Esta versão aprimora a AWS Service Catalog AppRegistry integração AWS Trusted Advisor e adiciona as `AWSWellArchitectedDis`	3 de maio de 2023

	`coveryServiceRoleP olicy` às políticas AWS gerenciadas.	
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
Atualizou a orientação do IAM para 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 AWS Trusted Advisor a AWS Service Catalog AppRegistry integração e.	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	Esta versão adiciona alterações de rastreamento para suas políticas AWS gerenciadas e adicionou uma nova ação para conceder a `ListAWSServiceAccessForOrganization` permissão ao`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 AWS Well-Architected no re:POST. 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
EventBridge suporte adicionado	AWS WA Tool agora envia um evento para a Amazon EventBridge quando uma alteração é feita em um recurso do Well-Architected.	3 de março de 2022
Lentes personalizadas adicionadas	A capacidade de adicionar lentes personalizadas foi adicionada.	29 de novembro de 2021
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	Esta versão adiciona a AWS WA Tool API. AWS CloudTrail informações de registro adicionadas.	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	O compartilhamento esclarecido do Regiões da AWS foi 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 sobre como AWS os usos de seus dados foram adicionados.	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	Esclareceu que os compartilhamentos da carga de trabalho são específicos 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 DeleteWorkload ação 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	Esta versão adiciona a capacidade de especificar não-Regiões da AWS ao definir uma carga de trabalho.	14 de fevereiro de 2019
AWS Well-Architected Tool disponibilidade geral	Esta versão apresenta o AWS Well-Architected Tool.	29 de novembro de 2018

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.