ユーザーガイド

AWS Well-Architected Tool

AWS Well-Architected Tool: ユーザーガイド

Table of Contents

AWS Well-Architected Tool Connector for Jira を使用して Jira アカウントを にリンクし AWS Well-Architected Tool、ワークロードと Jira プロジェクト間で改善項目を同期できます。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。

AWS Well-Architected Tool とは

AWS Well-Architected Tool (AWS WA Tool) は、AWS のベストプラクティスを使用してアーキテクチャを測定するための一貫したプロセスを提供するクラウド内のサービスです。AWS WA Tool は、次を実行することで製品ライフサイクル全体でサポートします。

- 決定事項のドキュメント化を支援する
- ベストプラクティスに基づいてワークロードを改善するための推奨事項を提供する
- ワークロードの信頼性、安全性、効率性、費用対効果の向上

AWS WA Tool を使用すると、AWS Well-Architected フレームワークのベストプラクティスを使用して、ワークロードを文書化して測定します。これらのベストプラクティスは、AWS ソリューションアーキテクトがさまざまなビジネスでソリューションを構築してきた長年の経験を基に開発されています。このフレームワークは、アーキテクチャを測定するための一貫したアプローチを提供します。また、時間の経過とともにニーズに応じてスケーリングする設計を実装するのに役立つガイダンスも提供します。

AWS のベストプラクティスに加えてカスタムレンズを使用することで、独自のベストプラクティスに照らしてワークロードを測定できます。カスタムレンズ内の質問は、特定のテクノロジーに特化したり、組織内のガバナンスニーズに対応したりできるようにカスタマイズできます。カスタムレンズは、AWS レンズが提供するガイダンスを補足するものです。

AWS Trusted Advisor と AWS Service Catalog AppRegistry を統合することで、Well-Architected のレビューに関する質問に回答するために必要な情報をより簡単に見つけることができます。

このサービスは、最高技術責任者 (CTO)、アーキテクト、デベロッパー、運用チームのメンバーなど、技術的な製品開発に携わる方を対象としています。AWS のお客様は、アーキテクチャの文書化、製品起動のガバナンス、テクノロジーポートフォリオのリスクの把握と管理のために AWS WA Tool を利用しています。

トピック

- AWS Well-Architected フレームワーク
- 定義

AWS Well-Architected フレームワーク

AWS Well-Architected フレームワークは、特定のアーキテクチャがクラウドのベストプラクティスにどの程度沿っているかを判断するための、一連の基本的な質問をドキュメント化しています。このフレームワークは、最新のクラウドベースのシステムに要求される品質に対してシステムを評価する一貫したアプローチを提供します。アーキテクチャの状態に基づいて、フレームワークはこれらの品質をより良く達成するために改善できることを提案します。

このフレームワークを使用することで、信頼性、セキュリティ、効率、コスト効果が高いシステムを設計し、クラウド内で運用するためのアーキテクチャのベストプラクティスを学習できます。また、このフレームワークは、ベストプラクティスに照らしてアーキテクチャを評価し、改善すべき分野を特定する一貫した方法を提供します。このフレームワークは、運用上の優秀性、セキュリティ、信頼性、パフォーマンス効率、コスト最適化および持続可能性という 6 本の柱を基本としています。

ワークロードの設計時には、ビジネスニーズに基づいてこれらの柱間でトレードオフを行います。これらのビジネス上の意思決定は、エンジニアリングの優先順位決定を促進する助けになります。開発環境では、信頼性を犠牲にして、コストを削減 (最適化) する場合があります。ミッションクリティカルなソリューションでは、コストの増加を受け入れて、信頼性を最適化する場合があります。e コマースソリューションでは、顧客満足度が収益の増加を促進する可能性があるため、パフォーマンスを優先する場合があります。セキュリティおよび運用上の優秀性は通常、他の柱に対してトレードオフされることはありません。

フレームワークの詳細については、AWSWell-Architected ウェブサイトを参照してください。

定義

AWS WA Tool および AWS Well-Architected フレームワークの場合:

- ワークロードでは、ビジネス価値をもたらす一連のコンポーネントが特定されます。ワークロードは通常、ビジネスとテクノロジーのリーダーが詳細に話し合う対象です。ワークロードの例には、マーケティングウェブサイト、e コマースウェブサイト、モバイルアプリのバックエンド、分析プラットフォームが含まれます。ワークロードは、アーキテクチャの複雑さのレベルによって異なります。静的ウェブサイトのようにシンプルなものになる場合も、複数のデータストアと多数のコンポーネントで構成されるマイクロサービスアーキテクチャのように複雑なものになる場合もあります。
- マイルストーンは、製品のライフサイクル (設計、テスト、稼働開始、本番稼働) を通じて進化するアーキテクチャの重要な変化を示すものです。

- レンズは、ベストプラクティスに照らしてアーキテクチャを評価し、改善すべき分野を特定する一貫した方法を提供します。

  AWS が提供するレンズに加えて、独自のレンズを作成して使用したり、共有されたレンズを使用したりすることもできます。
- 高リスクの問題 (HRI) は、ビジネスに重大な悪影響を及ぼす可能性があると AWS が認識した、アーキテクチャおよび運用上の選択肢です。HRI は、組織の運用、資産、個人に影響を及ぼす可能性があります。
- 中リスクの問題 (MRI) は、ビジネスに悪影響を及ぼす可能性があると AWS が認識した、アーキテクチャおよび運用上の選択肢ですが、その程度は HRI より低くなります。

  詳細については、「高リスクの問題 (HRI) と中リスクの問題 (MRI)」を参照してください。

はじめに AWS Well-Architected Tool

このセクションでは、の使用を開始する方法について説明します AWS WA Tool。

トピック

ユーザ、グループ、またはロールへのアクセスの提供 AWS WA Tool

このステップでは、 AWS WA Toolへのアクセスを許可します。

へのアクセスを提供します。 AWS WA Tool

1. アクセス権限を付与するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

   - 以下のユーザーとグループ AWS IAM Identity Center:

     アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

   - IAM 内で、ID プロバイダーによって管理されているユーザー:

     ID フェデレーションのロールを作成します。詳細については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールの作成」を参照してください。

   - IAM ユーザー:

     - ユーザーが担当できるロールを作成します。手順については、「IAM ユーザーガイド」の「IAM ユーザー用ロールの作成」を参照してください。

- (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加する。「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス許可の追加」の手順を実行します。

2. フルコントロールを許可するには、WellArchitectedConsoleFullAccess マネージドポリシーをアクセス許可一式またはロールに適用します。

   フルアクセス権限では、プリンシパルは内のすべてのアクションを実行できます AWS WA Tool。このアクセスは、ワークロードの定義、ワークロードの削除、ワークロードの表示、ワークロードの更新、ワークロードの共有、カスタムレンズの作成、カスタムレンズの共有に必要です。

3. 読み取り専用アクセスを許可するには、WellArchitectedConsoleReadOnlyAccess マネージドポリシーをアクセス許可セットまたはロールに適用します。このロールを持つプリンシパルは、リソースを表示することしかできません。

これらのポリシーの詳細については、「AWS の マネージドポリシー AWS Well-Architected Tool」を参照してください。

他の AWS サービスのサポートを有効化

組織アクセスを有効にすると、 AWS WA Tool 組織の構造に関する情報を収集して、リソースをより簡単に共有できるようになります (the section called “AWS Organizations 内でリソース共有を有効にする”詳細については、を参照してください)。Discovery サポートを有効にするとAWS Trusted Advisor、AWS Service Catalog AppRegistry、および関連リソース (AWS CloudFormation AppRegistry リソースコレクション内のスタックなど) から情報が収集され、Well-Architected によるレビューの質問に回答したり、ワークロードに合わせてチェックを調整したりするのに必要な情報をより簡単に見つけられるようになります。 Trusted Advisor

Discovery サポートを有効にしたり AWS Organizations、Discovery サポートを有効にしたりすると、アカウントにサービスにリンクされたロールが自動的に作成されます。

AWS WA Tool 連携できる他のサービスのサポートを有効にするには、[設定] に移動します。

1. 情報を収集するには AWS Organizations、[AWS Organizations サポートを有効にする] をオンにしてください。
2. [Discovery サポートの有効化] をオンにすると、その他 AWS サービスとリソースから情報を収集できます。

3. [ロールの許可を表示] を選択して、サービスにリンクされたロールアクセス許可または信頼関係ポリシーを確認します。
4. [設定を保存] を選択します。

AppRegistry ワークロードのアクティベーションを行う

AppRegistry 使用はオプションであり、 AWS ビジネスSupport およびエンタープライズサポートのお客様はワークロードごとに有効化できます。

Discovery サポートが有効になり、 AppRegistry 新規または既存のワークロードに関連付けられると、 AWS WA Tool サービス管理属性グループが作成されます。の属性グループ Metadata AppRegistry には、ワークロード ARN、ワークロード名、およびワークロードに関連するリスクが含まれます。

- Discovery サポートをオンにすると、ワークロードが変更されるたびに、属性グループが更新されます。
- Discovery サポートがオフになるか、アプリケーションがワークロードから削除されると、ワークロード情報は AWS Service Catalogから削除されます。

AppRegistry 取得したデータをアプリケーションに制御させたい場合は Trusted Advisor、ワークロードのリソース定義を「すべて」AppRegistryまたは「すべて」に設定します。the section called “IAM でのアクティベーション Trusted Advisor ” のガイドラインに従って、アプリケーションでリソースを保有するすべてのアカウントに対するロールを作成します。

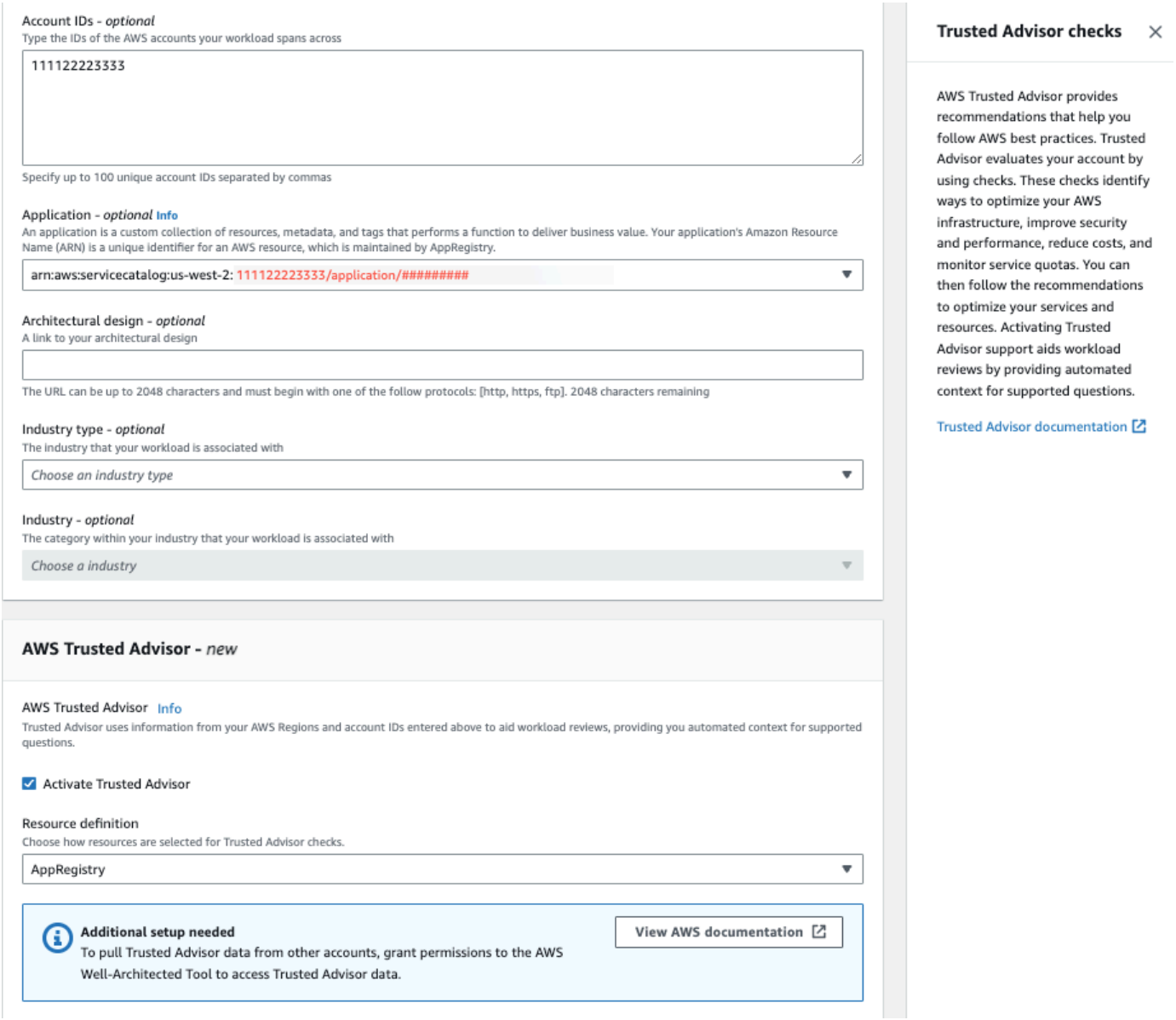
AWS Trusted Advisor ワークロードのアクティベーション

AWS Trusted Advisor との統合はオプションであり、 AWS ビジネスSupport およびエンタープライズサポートのお客様はワークロードごとに有効化できます。 Trusted Advisor との統合には費用はかかりませんが AWS WA Tool、 Trusted Advisor 料金の詳細については、「AWS Support プラン」を参照してください。

ワークロードの Trusted Advisor をアクティブ化する

1. 有効化するには Trusted Advisor、ワークロード所有者は既存のワークロードを更新するか、「Define workload」を選択して新しいワークロードを作成できます。 AWS WA Tool
2. 使用するアカウント ID を [Account ID] フィールドに入力するか、[Application] フィールドでアプリケーション ARN を選択するか、または両方を選択してアクティブ化します Trusted Advisor。 Trusted Advisor

3. [AWS Trusted Advisor] セクションで [Trusted Advisorをアクティブ化する] を選択します。



4. IAM Trusted Advisor サービスロールが作成されるという通知は、ワークロードが初めてアクティブ化されたときに表示されます。[許可を表示] を選択すると、IAM ロールのアクセス許可が表示されます。JSON が IAM で自動作成したロール名、アクセス許可および信頼関係を閲覧できます。ロールが作成されたら、 Trusted Advisor をアクティブ化する後続のワークロードでは、[追加のセットアップが必要です] という通知が表示されます。

5. 「リソース定義」ドロップダウンでは、「ワークロードメタデータ」または「すべて」を選択できます。AppRegistryリソース定義の選択では、Well-Architected AWS WA Tool のベストプラクティスに対応するワークロードレビューのステータスチェックを行うためにどのデータを取得するかを定義します。 Trusted Advisor

ワークロードメタデータ — ワークロードはアカウント ID によって定義され、 AWS リージョンワークロード内で指定されます。

AppRegistry— ワークロードは、 AppRegistry ワークロードに関連するアプリケーションに存在するリソース (AWS CloudFormation スタックなど) によって定義されます。

すべて — AppRegistry ワークロードはワークロードのメタデータとリソースの両方によって定義されます。

6. [次へ] をクリックします。
7. AWS Well-Architected フレームワークをワークロードに適用し、[ワークロードの定義] を選択します。 Trusted Advisor AWS チェックはWell-Architected Frameworkにのみリンクされており、他のレンズにはリンクされていません。

は IAM AWS WA Tool Trusted Advisor で作成されたロールを使用して定期的にデータを取得します。IAM ロールはワークロード所有者用に自動作成されます。ただし、 Trusted Advisor 情報を表示するには、ワークロード上の関連アカウントの所有者が IAM にアクセスしてロールを作成する必要があります。詳細については、「???」を参照してください。このロールが存在しない場合、 AWS WA Tool Trusted Advisor そのアカウントの情報を取得できず、エラーが表示されます。

AWS Identity and Access Management (IAM) でのロール作成の詳細については、『IAM ユーザーガイド』の「 AWS サービスのロールの作成 (コンソール)」を参照してください。

IAM Trusted Advisor でのワークロードのアクティベーション

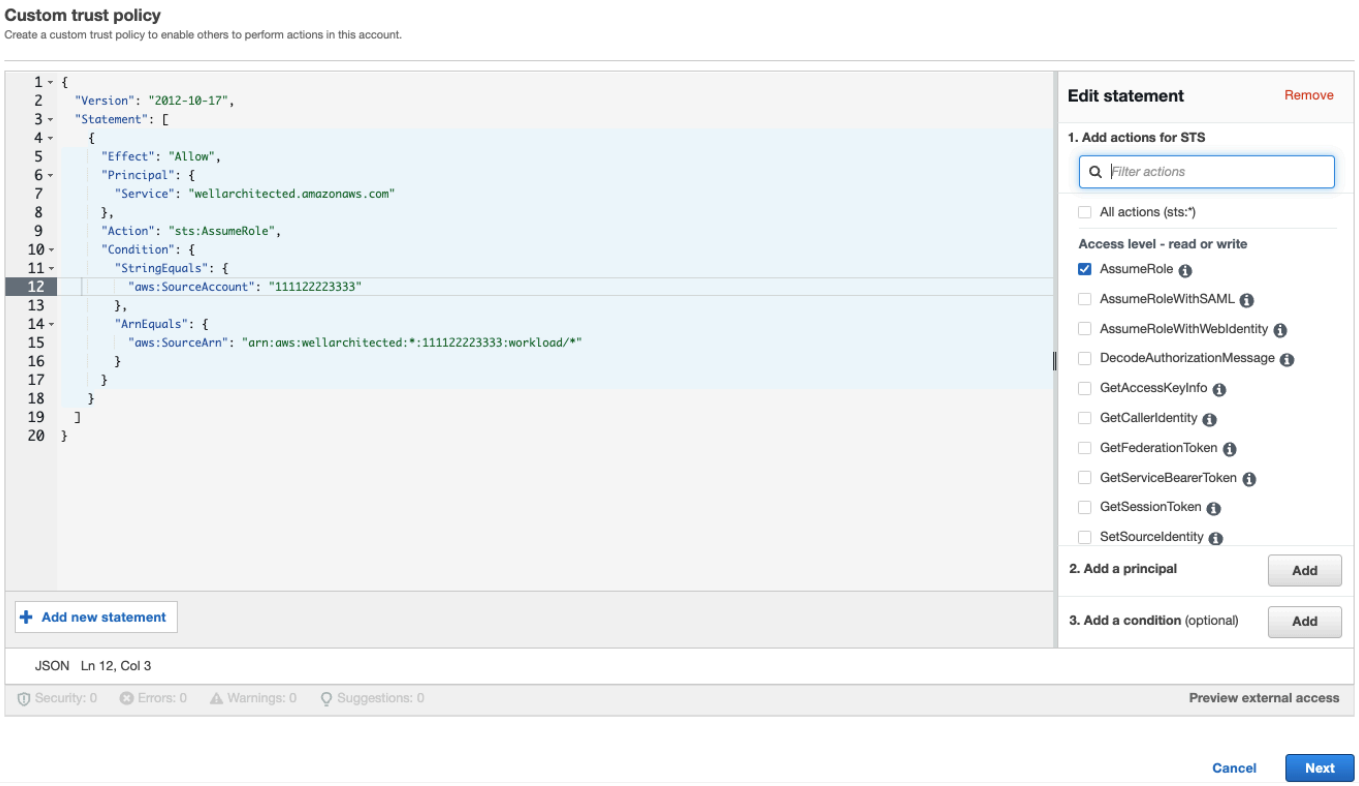
> **Note**
>
> ワークロードの所有者は、ワークロードを作成する前に、自分のアカウントの Discovery サポートを有効化する必要があります。 Trusted Advisor [Discovery サポートの有効化] を選択すると、ワークロード所有者に必要なロールが作成されます。他のすべての関連アカウントには、以下の手順を使用してください。

有効化されたワークロードの関連アカウントのオーナーは、IAM Trusted Advisor Trusted Advisor でロールを作成して情報を確認する必要があります。 AWS WA Tool

IAM AWS WA Tool で情報を取得するためのロールを作成するには Trusted Advisor

1. AWS Management Console にサインインし、で IAM コンソールを開きます。https://console.aws.amazon.com/iam/
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] の順に選択します。
3. [信頼されたエンティティのタイプ] で、[カスタム信頼ポリシー] を選択します。
4. 次の図に示すように、次のカスタム信頼ポリシーをコピーして IAM コンソールの JSON フィールドに貼り付けます。*WORKLOAD_OWNER_ACCOUNT_ID* をワークロード所有者のアカウント ID に置き換え、[次へ] を選択します。

```
{
  "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

aws:sourceArn前述のカスタム信頼ポリシーの条件ブロックにある「」は"arn:aws:wellarchitected:*:*WORKLOAD_OWNER_ACCOUNT_ID*:workload/*"、このロールをワークロード所有者のすべてのワークロードに使用できることを示す一般的な条件です。 AWS WA Tool ただし、アクセスを特定のワークロード ARN または一連のワークロード ARN に絞り込むことができます。複数の ARN を指定するには、次の信頼ポリシーの例を参照してください。

```
{
    "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. 「権限の追加」ページの「 AWS WA Tool アクセス権限ポリシー」で、「ポリシーの作成」を選択してデータの読み取り権限を付与します。 Trusted Advisor[ポリシーの作成] を選択すると、新しいウィンドウが開きます。

> **Note**
>
> さらに、ロール作成中はアクセス許可の作成を省略し、ロールの作成後にインラインポリシーを作成することもできます。ロールが正常に作成された旨を示すメッセージで [ロールを表示] を選択し、[アクセス許可] タブの [アクセス許可の追加] ドロップダウンから [インラインポリシーの作成] を選択します。

6. 以下のアクセス許可ポリシーをコピーして、[JSON] フィールドに貼り付けます。Resource ARN で、*YOUR_ACCOUNT_ID* を自分のアカウント ID に置き換え、リージョンまたはアスタリスク (*) を指定して、[次へ: タグ] を選択します。

   ARN 形式の詳細については、「AWS の一般的なリファレンスガイド」の「Amazon リソースネーム (ARN)」を参照してください。

```
{
    "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. Trusted Advisor がワークロードに対して有効化され、リソース定義が「すべて」AppRegistryに設定されている場合、 AppRegistry ワークロードにアタッチされたアプリケーション内のリソースを所有するすべてのアカウントは、 Trusted Advisor 以下の権限をロールの権限ポリシーに追加する必要があります。

```
{
    "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. (オプション) タグを追加します。[次へ: レビュー] を選択します。
9. ポリシーが正しいことを確認したら、名前を付けて、[ポリシーの作成] を選択します。

10. ロールの [アクセス許可の追加] ページで、作成したポリシー名を選択し、[次へ] を選択します。
11. `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* の構文に沿ったロール名を入力し、[ロールを作成] を選択します。*`WORKLOAD_OWNER_ACCOUNT_ID`* をワークロード所有者のアカウント ID に置き換えます。

    ページ上部にロールが正常に作成されたことを知らせるメッセージが表示されます。
12. ロールと関連するアクセス許可ポリシーを表示するには、左側のナビゲーションペインの [アクセス管理] で [ロール] を選択し、`WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* の名前を検索します。ロールの名前を選択して、[アクセス許可] と [信頼関係] が正しいことを確認します。

Trusted Advisor ワークロードの非アクティブ化

ワークロードの Trusted Advisor を非アクティブ化するには

ワークロードを編集して [Activate] Trusted Advisor AWS WA Tool を選択解除することで、からどのワークロードでも非アクティブ化できます。 Trusted Advisorワークロードの編集に関する詳細は、「the section called “ワークロードの編集”」を参照してください。

Trusted Advisor AWS WA Tool から非アクティブ化しても、IAM で作成されたロールは削除されません。IAM からロールを削除するには、別のクリーンアップ手段が必要です。ワークロードの所有者または関連するアカウントの所有者は、 Trusted Advisor で非アクティブ化されたときに作成された IAM ロールを削除するか AWS WA Tool、 AWS WA Tool Trusted Advisor ワークロードのデータ収集を停止する必要があります。

IAM で **`WellArchitectedRoleForTrustedAdvisor`** を削除するには

1. AWS Management Console にサインインし、で IAM コンソールを開きます。https://console.aws.amazon.com/iam/
2. IAM コンソールのナビゲーションペインで、[ロール] を選択します。
3. `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* を検索して、ロール名を選択します。
4. [削除] を選択します。ポップアップウィンドウで、ロール名を入力して削除を確認したら、もう一度 [削除] を選択します。

IAM からロールを削除する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの削除 (コンソール)」を参照してください。

ワークロードの定義

次の手順では、ワークロードを定義します。

ワークロードを定義するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool にあるコンソールを開きます。
2. 初めて使用する場合は AWS WA Tool、サービスの機能を紹介するページが表示されます。[ワークロードを定義する] セクションで [ワークロードの定義] を選択します。

   あるいは、左側のナビゲーションペインで、[Workloads (ワークロード)]、[Define workload (ワークロードの定義)] の順に選択します。

   AWS ワークロードデータの使用方法の詳細については、「 AWS このデータが必要な理由と使用方法」を選択してください。
3. [Name (名前)] ボックスに、ワークロードの名前を入力します。

   > **Note**
   >
   > 名前は 3 ~ 100 文字にします。3 文字以上をスペースにしないでください。ワークロード名は一意にしてください。一意かどうかを確認するときは、スペースと大文字は無視されます。
4. [Description (説明)] ボックスに、ワークロードの説明を入力します。説明は 3 ~ 250 文字にしてください。
5. [Review owner (レビューの 所有者)] ボックスに、ワークロードのレビュープロセスを所有するプライマリグループまたは個人の名前、E メールアドレス、または識別子を入力します。
6. [環境] ボックスで、ワークロードの環境を選択します。
   - [Production] (本番稼動) – ワークロードは本番稼動環境で実行されます。
   - [Pre-production] (本番稼働前) – ワークロードは本番稼働前環境で実行されます。
7. [リージョン] セクションで、ワークロードのリージョンを選択します。
   - AWS リージョン— AWS リージョン ワークロードを実行する場所を 1 つずつ選択します。

- AWS 非リージョン — AWS ワークロードが実行されている場所以外のリージョンの名前を入力します。5 つまでの一意のリージョンをカンマで区切って指定できます。

ワークロードに該当する場合は、両方のオプションを使用します。

8. (オプション) [Account IDs] (アカウント ID) ボックスに、ワークロードに関連付けられている AWS アカウント の ID を入力します。最大 100 個の一意のアカウント ID をカンマで区切って指定できます。

   を有効にすると、指定したアカウント ID がデータの取得に使用されます Trusted Advisor。Trusted Advisor IAM AWS Trusted AdvisorAWS WA ToolTrusted Advisor 内でユーザーに代わってデータを取得するためのアクセス権限を付与するには、「ワークロードのアクティベーション」を参照してください。

9. (オプション) [アプリケーション] ボックスに、AWS Service Catalog AppRegistry からこのワークロードに関連付けるアプリケーションのアプリケーション ARN を入力します。各ワークロードに指定できる ARN はひとつだけで、アプリケーションとワークロードは、同じリージョンである必要があります。

10. (オプション) [Architectural design (アーキテクチャ設計)] ボックスに、アーキテクチャ設計の URL を入力します。

11. (オプション) [Industry type (業界)] ボックスで、ワークロードに関連する業界を選択します。

12. (オプション) [Industry (業種)] ボックスで、ワークロードに最も一致する業種を選択します。

13. (オプション) [Trusted Advisor] セクションで、ワークロードに対して [Trusted Advisor のチェック] をオンにし、[Trusted Advisorをアクティブ化する] を選択します。ワークロードに関連するアカウントには、追加の設定が必要な場合があります。the section called “アクティベーション Trusted Advisor” AWS WA Tool Trusted Advisor ユーザーに代わってデータを取得するためのアクセス権限を付与するにはを参照してください。 AWS WA Tool Trusted Advisor チェックの実行に使用するリソースを定義するにはAppRegistry、[ワークロードメタデータ] または [リソース定義] の [すべて] を選択します。

14. (オプション) Jira セクションで、ワークロードのワークロードレベルの Jira 同期設定を有効にするには、[アカウントレベル設定の上書き] を選択します。ワークロードに関連するアカウントには、追加の設定が必要な場合があります。AWS Well-Architected Tool コネクタの設定と構成を開始するには、「Jira 用コネクタ」を参照してください。[ワークロードを同期しない]、[ワークロードを同期 -手動]、および [ワークロードを同期-自動] から選択し、オプションで同期する Jira プロジェクトキーを入力します。

> **Note**
>
> アカウントレベルの設定を上書きしない場合、ワークロードはデフォルトでアカウントレベルの Jira 同期設定になります。

15. (オプション) [Tags] (タグ) セクションで、ワークロードに関連付けるタグを追加します。

    タグの詳細については、「AWS WA Tool リソースのタグ付け」を参照してください。

16. [次へ] をクリックします。

    必須ボックスが空白の場合、または指定した値が無効な場合は、続行する前に問題を修正する必要があります。

17. (オプション) [プロファイルの適用] で、既存のプロファイルを選択するか、プロファイル名を検索するか、[プロファイルの作成] を選択してプロファイルを作成し、プロファイルをワークロードに関連付けます。[次へ] をクリックします。

18. このワークロードに適用するレンズを選択します。ワークロードには最大 20 個のレンズを追加できます。公式レンズの説明については、「レンズ」を参照してください。 AWS

    レンズは、カスタムレンズ (自分で作成したレンズまたは共有したレンズ AWS アカウント)、レンズカタログ (AWS すべてのユーザーが利用できる公式レンズ)、またはその両方から選択できます。

> **Note**
>
> カスタムレンズを作成していない場合や、カスタムレンズを共有していない場合、[カスタムレンズ] セクションには何も表示されません。

> **免責事項**
>
> 他のユーザーまたはアカウントが作成したカスタムレンズにアクセスしたり、 AWS 他のユーザーまたはアカウントが作成したカスタムレンズを適用したりすることで、AWS 他のユーザーが作成して共有したカスタムレンズが顧客契約で定義されている第三者コンテンツであることを認めたものとみなされます。

19. [ワークロードの定義] を選択します。

必須ボックスが空白の場合、または指定した値が無効な場合は、ワークロードを定義する前に問題を修正する必要があります。

ワークロードのドキュメント化

ワークロードを定義したら、その状態をドキュメント化します。

ワークロードの状態をドキュメント化するには

1. 最初にワークロードを定義すると、ワークロードの現在の詳細を示すページが表示されます。[Start reviewing (レビューの開始)] を選択して開始します。

   それ以外の場合は、左側のナビゲーションペインで [Workloads (ワークロード)] を選択してから、ワークロードの名前を選択して、ワークロード詳細ページを開きます。[Continue reviewing (確認を続行)] を選択します。

   (オプション) プロファイルがワークロードに関連付けられている場合、左側のナビゲーションペインには、ワークロードレビュープロセスを加速するために使用できる優先度の高いワークロードレビューの質問リストが表示されます。
2. 最初の質問が表示されます。質問ごとに、以下の手順を実行します。

   a. 質問を読み、質問がワークロードに当てはまるかどうかを判断します。

      その他のガイダンスについては、[情報] を選択すると、ヘルプパネルに情報が表示されます。

      - 質問がワークロードに当てはまらない場合は、[Question does not apply to this workload (質問はこのワークロードに当てはまらない)] を選択します。
      - それ以外の場合は、リストから現在従っているベストプラクティスを選択します。

        現在どのベストプラクティスにも従っていない場合は、[None of these (該当なし)] を選択します。

      任意の項目に関するその他のガイダンスについては、[情報] を選択すると、ヘルプパネルに情報が表示されます。

   b. (オプション) 1 つ以上のベストプラクティスがワークロードに適用されない場合は、[Mark best practice(s) that don't apply to this workload] (このワークロードに適用されないベストプ

ラクティスをマーク) を選択します。選択したベストプラクティスごとに、オプションで理由を選択し、追加の詳細を指定できます。

c. (オプション) 質問に関する情報を記録するには、[コメント] ボックスを使用します。

たとえば、質問が当てはまらない理由を説明したり、選択したベストプラクティスに関する追加の詳細を提供したりできます。

d. 次の質問に進むには [Next (次へ)] を選択します。

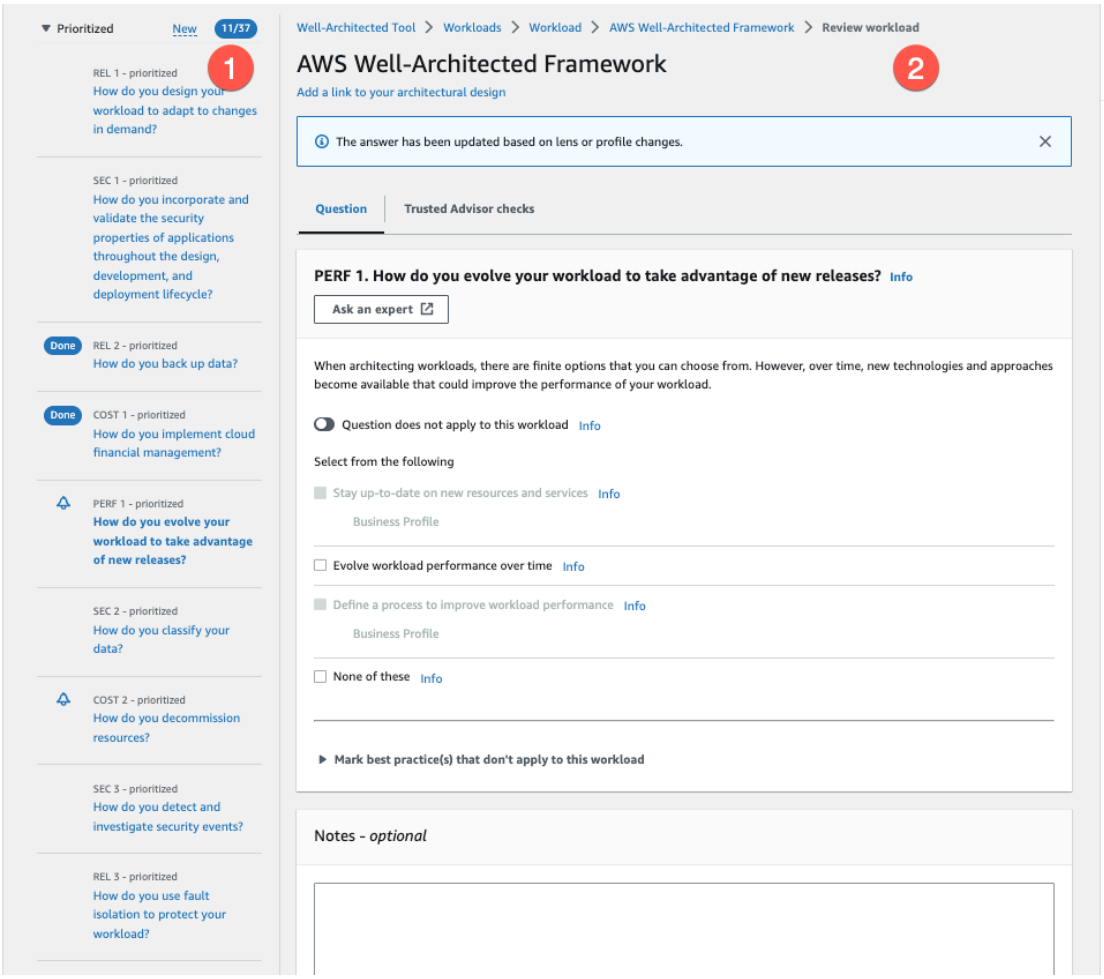
各柱の質問ごとにこれらの手順を繰り返します。

3. 変更を保存し、ワークロードのドキュメント化を一時停止するときは、いつでも [Save and exit (保存して修了)] を選択します。

質問に戻るには、ワークロード詳細ページに移動し、[Continue reviewing (レビューの続行)] を選択します。

[ワークロードのレビュー] ページ

[ワークロードのレビュー] ページには、3 つのペインがあります。



1. 左側のナビゲーションペインには、各柱に関する質問が表示されます。回答した質問には [Done] (完了) と表示されます。各柱の回答された質問の数は柱の名前の横に表示されます。

   他の柱の質問に移動するには、その柱の名前を選択してから回答する質問を選択します。

   (オプション) プロファイルがワークロードに関連付けられている場合は、 AWS WA Tool はプロファイル内の情報を使用して、ワークロードレビューのどの質問の優先度が高いか、そしてどの質問がユーザーのビジネスに該当しないのかを判断します。左側のナビゲーションペインで、優先度が高い質問を使用するとワークロードレビュープロセスを加速できます。優先度の高い質問のリストに新しく追加された質問の横には、通知アイコンが表示されます。
2. 中央のペインには、現在の質問が表示されます。従っているベストプラクティスを選択します。質問に関する詳細やベストプラクティスを入手するには、[Info (情報)] を選択します。「エキスパートに聞く」を選択して、Well-Architected 専用の AWS re: Post コミュニティにアクセスしてください。AWS AWS re: POST はフォーラムに代わるトピックベースのコミュニティです。question-and-answer AWS re: POST では、回答を検索したり、質問に回答したり、グループに参加したり、人気のトピックをフォローしたり、お気に入りの質問や回答に投票したりできます。

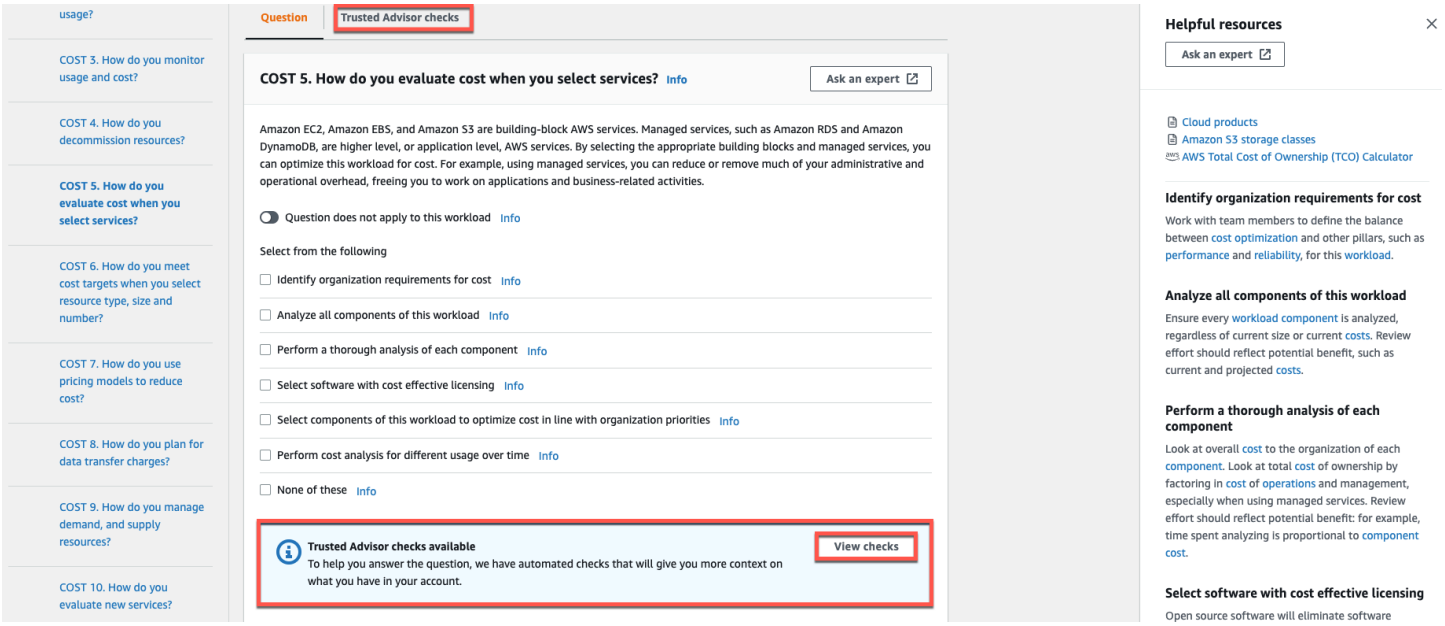
(オプション) 1 つ以上のベストプラクティスを非適用としてマークするには、[このワークロードに適用されないベストプラクティスをマーク] を選択して、適用されないベストプラクティスを選択します。

このペインの下部にあるボタンを使用して、次の質問に進むか、前の質問に戻るか、変更内容を保存して終了します。

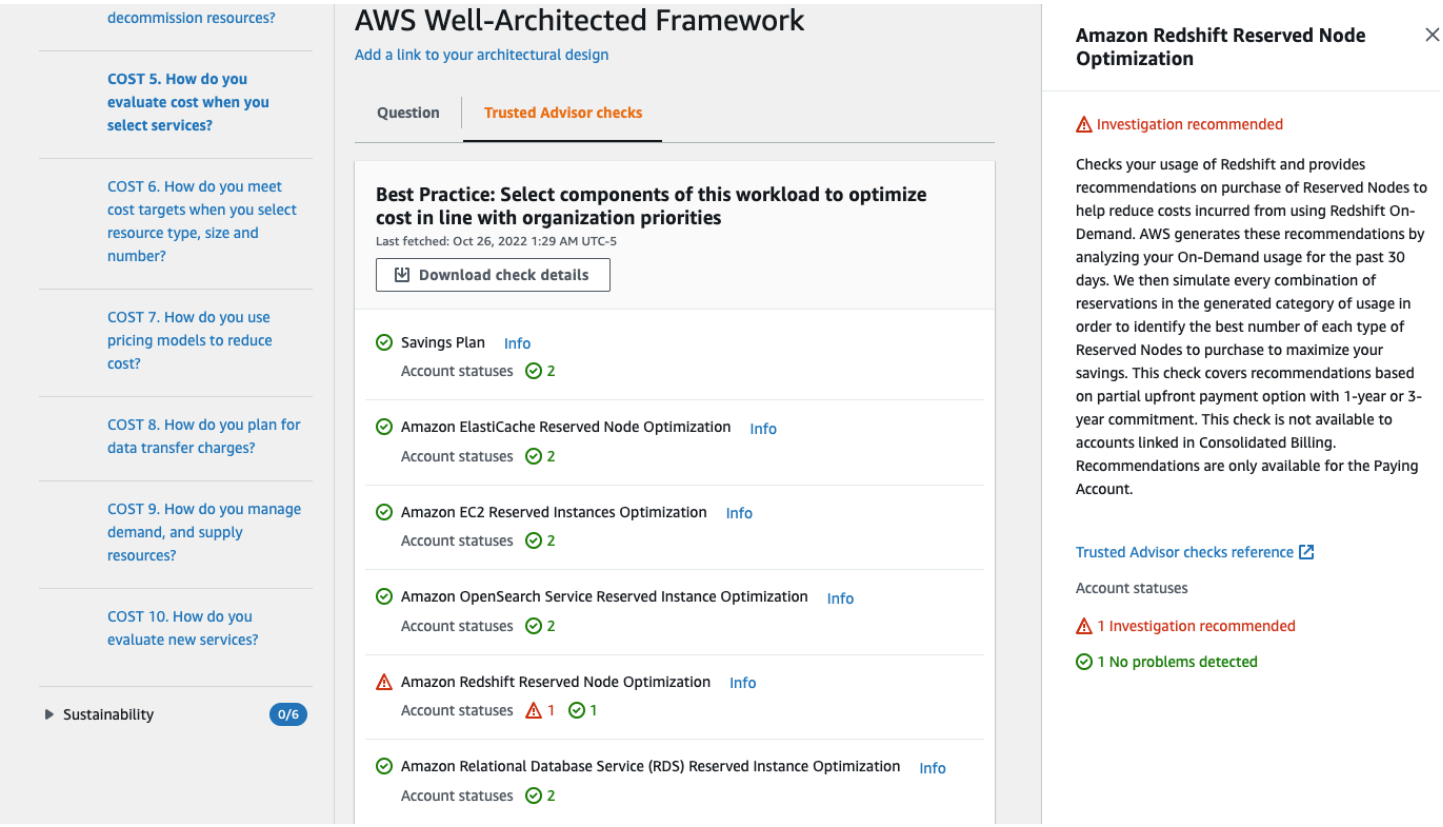
3. 右側のペインに、詳細と役立つリソースが表示されます。「エキスパートに聞く」を選択して、Well-Architected 専用の AWS re: Post コミュニティにアクセスしてください。AWSこのコミュニティでは、 AWSのワークロードの設計、構築、デプロイ、運用に関する質問をすることができます。

Trusted Advisor チェック

Trusted Advisor ワークロードでが有効になっている場合は、Question Trusted Advisor の横にチェックタブが表示されます。ベスト・プラクティスに該当するチェックがある場合は、質問の選択の後に、 Trusted Advisor 利用可能なチェックがあるという通知が表示されます。[チェックを表示] を選択すると、[Trusted Advisor のチェック] タブに移動します。



[Trusted Advisor チェック] タブでは、ベストプラクティスのチェックに関する詳細情報を確認したり Trusted Advisor、[ヘルプリソース] Trusted Advisor ペインのドキュメントへのリンクを表示したり、 Trusted Advisor 各ベストプラクティスのチェックとステータスのレポートを CSV ファイルで提供するチェックの詳細をダウンロードしたりできます。



Trusted Advisor のチェックカテゴリは色付きのアイコンで表示され、各アイコンの横の数字はそのステータスのアカウント数を示しています。

- 推奨アクション (赤) — Trusted Advisor チェックのアクションを推奨します。
- 調査推奨 (黄色) — Trusted Advisor チェックで発生する可能性のある問題を検出します。
- 問題は検出されませんでした (緑) Trusted Advisor — チェックの対象となる問題は検出されませんでした。
- [非表示の項目 (グレー)] — チェックで無視するリソースなど、除外項目があるチェックの数。

Trusted Advisor 提供されるチェックについて詳しくは、『AWS Support ユーザーガイド』の「チェックカテゴリーを表示する」を参照してください。

Trusted Advisor 各チェックの横にある「情報」リンクを選択すると、そのチェックに関する情報がヘルプリソースペインに表示されます。詳細については、「AWS Support ユーザーガイド」の「AWS Trusted Advisor のチェックに関するリファレンス」を参照してください。

マイルストーンの保存

マイルストーンはいつでも保存できます。マイルストーンには、ワークロードの現在のステータスが記録されます。

マイルストーンを保存するには

1. ワークロード詳細ページで、[Save milestone (マイルストーンの保存)] を選択します。
2. [Milestone name (マイルストーン名)] ボックスに、マイルストーンの名前を入力します。

   > **Note**
   >
   > 名前は 3 ~ 100 文字にします。3 文字以上をスペースにしないでください。ワークロードに関連付けられるマイルストーン名は一意にしてください。一意かどうかを確認するときは、スペースと大文字は無視されます。

3. [保存] を選択します。

マイルストーンを保存した後は、そのマイルストーンに記録されたワークロードデータを変更することはできません。

詳細については、「マイルストーン」を参照してください。

チュートリアル

このチュートリアルでは AWS Well-Architected Tool 、を使用してワークロードを文書化し、測定する方法について説明します。この例では、小売 e コマースウェブサイトのワークロードを定義してドキュメント化する方法を順を追って説明します。

トピック

手順 1: ワークロードを定義する

まず、ワークロードを定義します。ワークロードを定義するには 2 つの方法があります。このチュートリアルでは、レビューテンプレートからワークロードを定義しません。レビューテンプレートからワークロードを定義する方法の詳細については、「the section called “ワークロードの定義”」を参照してください。

ワークロードを定義するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool のコンソールを開きます。

   > **Note**
   >
   > ワークロードの状態を文書化するユーザーは、 AWS WA Toolへの完全なアクセス許可を保持している必要があります。

2. [ワークロードを定義する] セクションで、[ワークロードの定義] を選択します。
3. [名前] ボックスに、ワークロード名として **`Retail Website - North America`** と入力します。
4. [Description (説明)] ボックスに、ワークロードの説明を入力します。
5. [レビューの所有者] ボックスに、ワークロードのレビュープロセスの担当者名を入力します。
6. [環境] ボックスで、ワークロードが本運用環境にあることを示します。

7. 私たちのワークロードは、 AWS 両方とローカルデータセンターの両方で実行されています。

    a. [AWS リージョン] を選択し、ワークロードが実行される北米の 2 つのリージョンを選択します。

    b. また、「AWS Non-#-region」を選択し、ローカルデータセンターの名前を入力します。

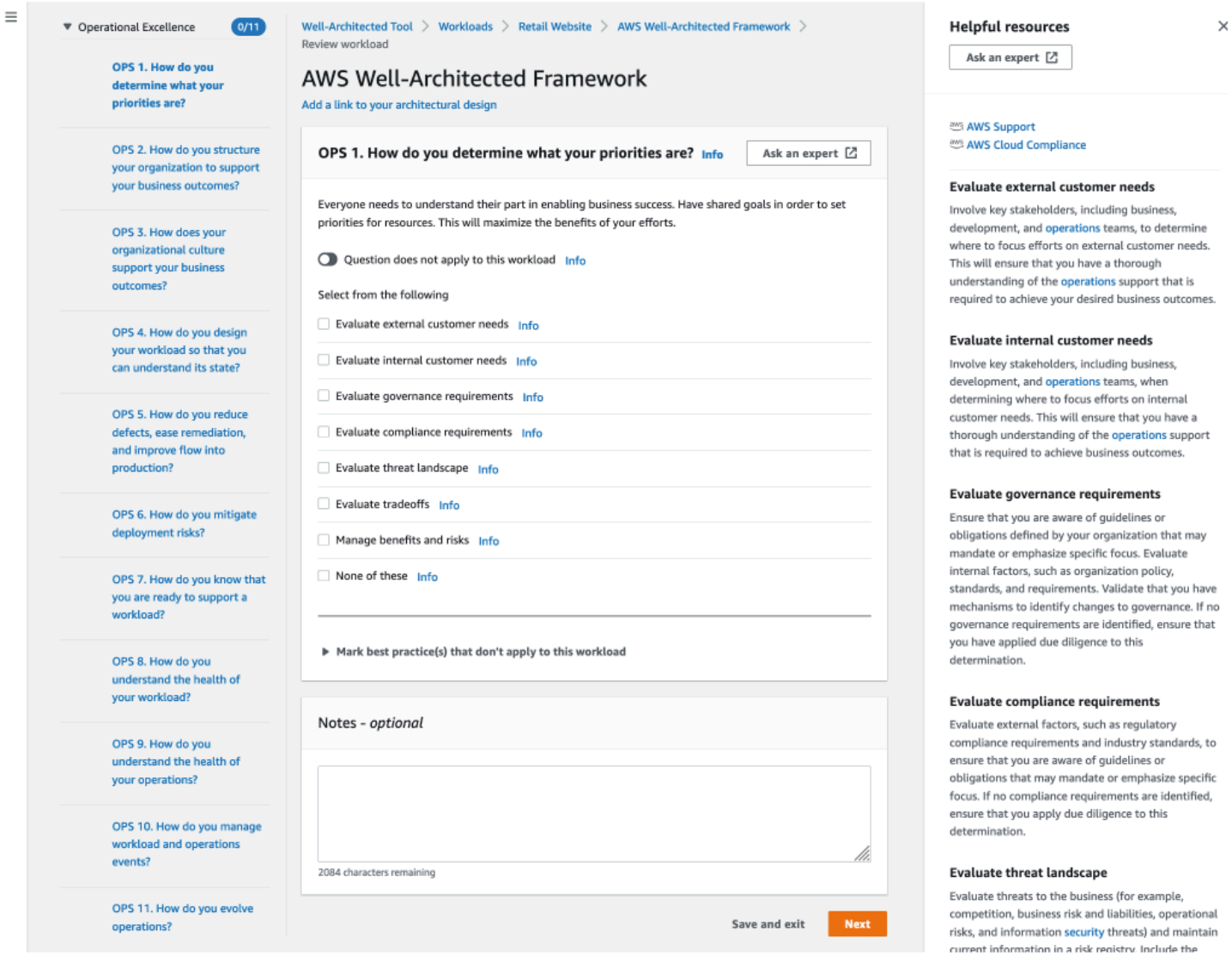
8. [アカウント ID] ボックスはオプションです。このワークロードには どの AWS アカウント も関連付けないでください。
9. [アプリケーション] ボックスはオプションです。このワークロードにアプリケーション ARN は入力しないでください。
10. [アーキテクチャ図] ボックスはオプションです。このワークロードにアーキテクチャ図を関連付けないでください。
11. [Industry type (産業タイプ)] ボックスと [Industry (産業)] ボックスはオプションで、このワークロードには指定されていません。
12. Trusted Advisor セクションはオプションです。このワークロードに対して、 Trusted Advisor サポートを有効化しないでください。
13. Jira セクションはオプションです。このワークロードの Jira セクションのアカウントレベルの設定を上書きしないでください。
14. この例では、ワークロードにタグを適用していません。[次へ] をクリックします。
15. [プロファイルの適用] 手順はオプションです。このワークロードにプロファイルを適用しないでください。[次へ] をクリックします。
16. この例では、自動的に選択される AWS Well-Architected Framework レンズを適用します。[Define workload (ワークロードの定義)] を選択して、これらの値を保存し、ワークロードを定義します。
17. ワークロードを定義したら、[Start reviewing (レビューの開始)] を選択してワークロードの状態のドキュメント化を開始します。

手順 2: ワークロードの状態を文書化する

ワークロードの状態を文書化するために、 AWS Well-Architected Frameworkの柱であるオペレーショナル・エクセレンス、セキュリティ、信頼性、パフォーマンス効率、コスト最適化、持続可能性に関する質問が提示されます。

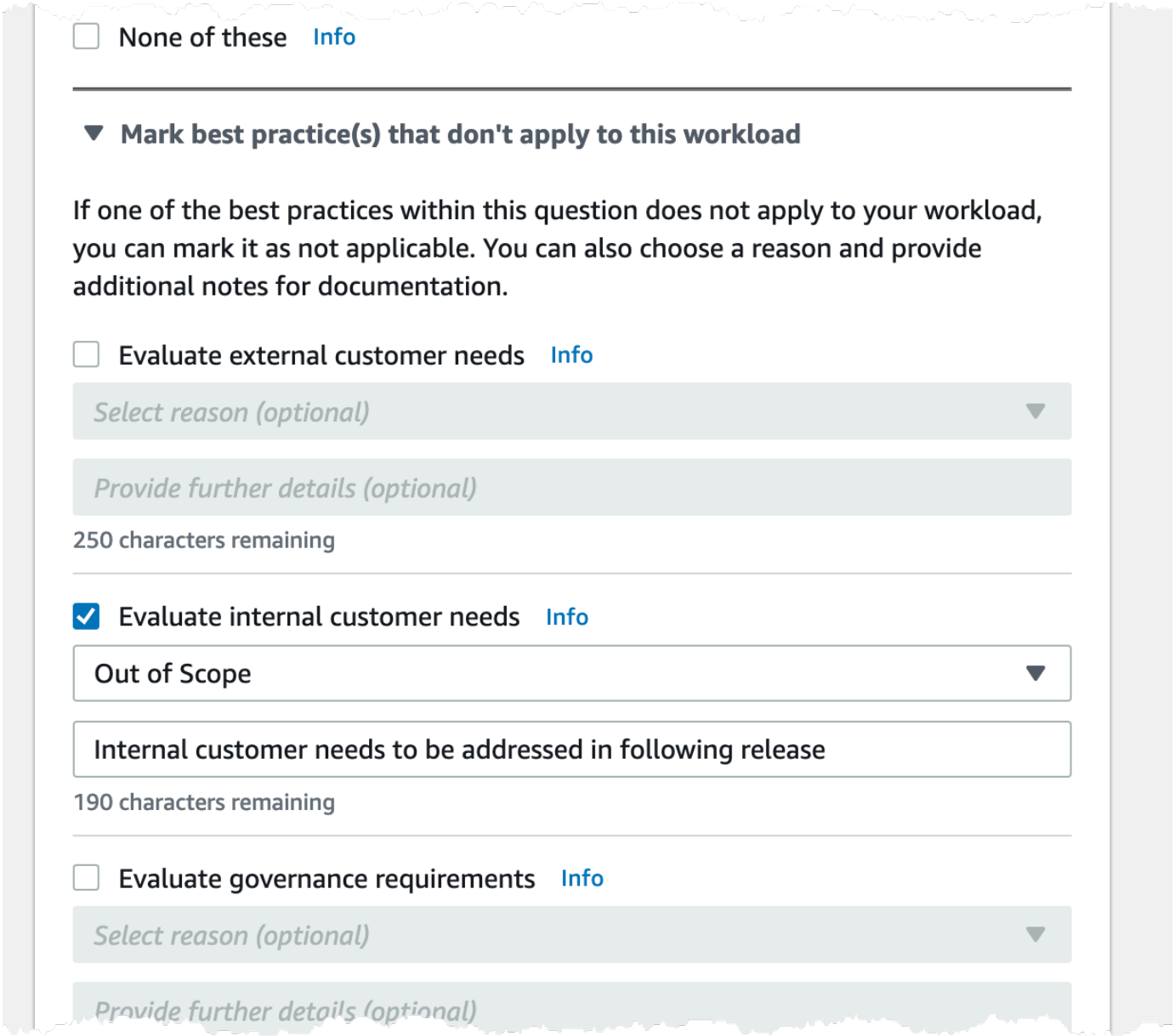
質問ごとに、表示されるリストからお客様が従っているベストプラクティスを選択します。ベストプラクティスに関する詳細が必要な場合は、[Info (情報)] を選択すると、右側のパネルに詳細とリソースが表示されます。

「エキスパートに聞く」を選択して、Well-Architected 専用の AWS re: Post コミュニティにアクセスしてください。AWSこのコミュニティでは、 AWSのワークロードの設計、構築、デプロイ、運用に関する質問をすることができます。



1. 次の質問に進むには [Next (次へ)] を選択します。左側のパネルを使用して、同じ柱の別の質問、または別の柱の質問に移動できます。
2. 「質問はこのワークロードには当てはまらない」または「どれにも当てはまらない」を選択した場合は、 AWS その理由をメモ欄に記入することをおすすめします。これらのコメントはワークロードレポートの一部として含まれ、今後、ワークロードに変更を加えるときに役立つことがあります。

> **Note**
>
> オプションで、1 つ以上の個々のベストプラクティスを適用しないものとしてマークできます。[Mark best practice(s) that don't apply to this workload] (このワークロードに適用されないベストプラクティスをマーク) を選択し、適用されないベストプラクティスを選択します。オプションで理由を選択し、追加の詳細を入力できます。適用されないベストプラクティスごとにこれを繰り返します。



> **Note**
>
> この処理は、[Save and exit] を選択していつでも一時停止できます。後で再開するには、 AWS WA Tool コンソールを開いて左側のナビゲーションペインで [Workloads] を選択します。

3. ワークロードの名前を選択して、ワークロードの詳細ページを開きます。
4. [Continue reviewing (レビューを続ける)] を選択すると、中断した場所に移動します。
5. すべての質問を完了すると、ワークロードの概要ページが表示されます。今すぐこれらの詳細をレビューできます。または、後で左側のナビゲーションペインで [Workloads (ワークロード)] を選択し、ワークロード名を選択して詳細に移動できます。

ワークロードの状態を初めてドキュメント化した後、マイルストーンを保存してワークロードレポートを生成する必要があります。

マイルストーンにはワークロードの現在の状態が記録されるため、改善計画に基づいて変更を加えながら進捗状況を評価できます。

[ワークロードの詳細] ページから:

1. [ワークロードの概要] セクションで、[マイルストーンを保存] ボタンを選択します。
2. マイルストーン名として **`Version 1.0 - initial review`** と入力します。
3. [保存] を選択します。
4. ワークロードレポートを生成するには、目的のレンズを選択します。[Generate report (レポートの生成)] を選択すると、PDF ファイルが作成されます。このファイルには、ワークロードの状態、特定されたリスクの数、推奨される改善点のリストが含まれています。

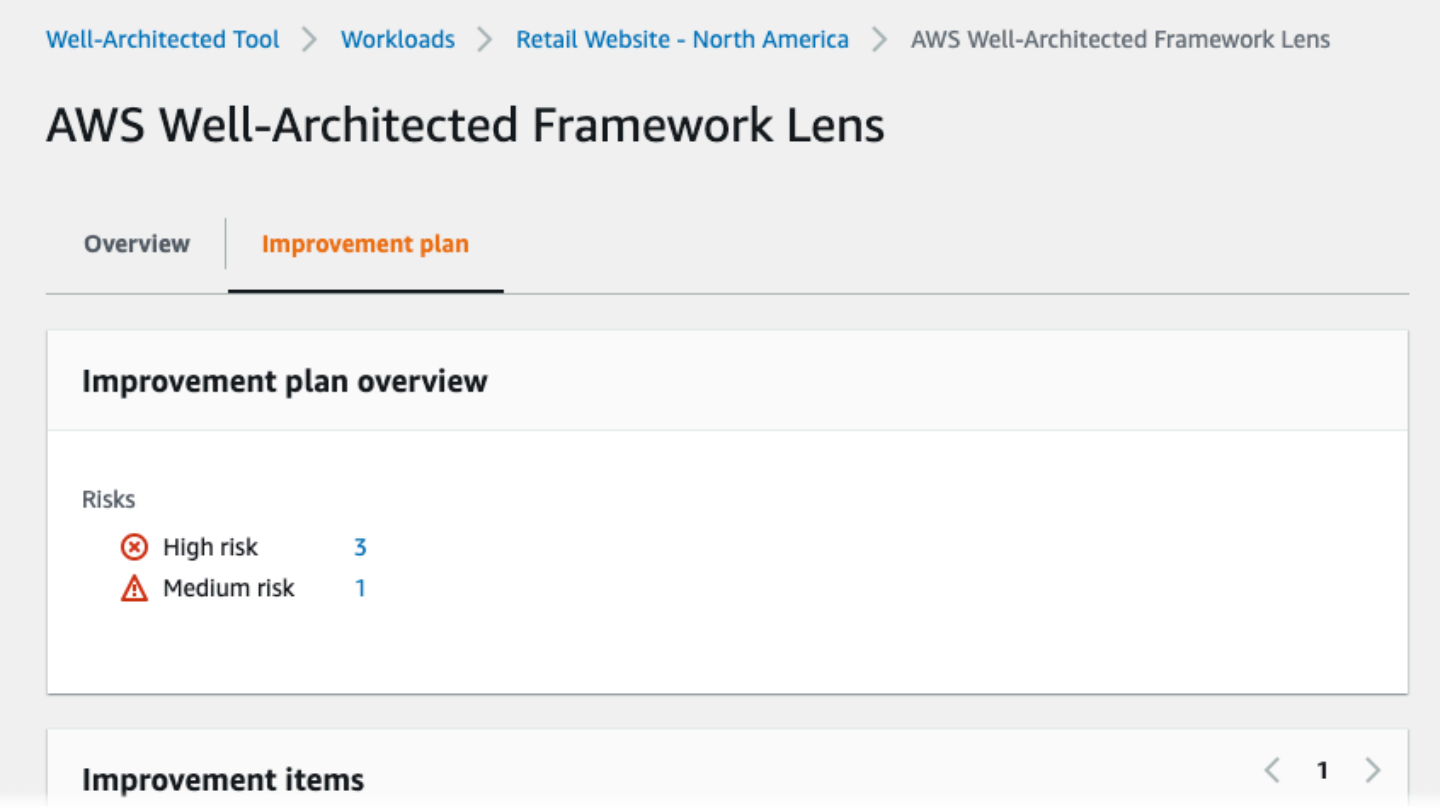
手順 3: 改善計画をレビューする

選択したベストプラクティスに基づいて、 AWS Well-Architected Framework AWS WA Tool Lensに照らして高リスクと中リスクの領域を特定します。

改善計画をレビューするには:

1. [概要] ページの [レンズ] セクションで、[AWS Well-Architected フレームワーク] を選択します。
2. 次に、[Improvement plan (改善計画)] を選択します。

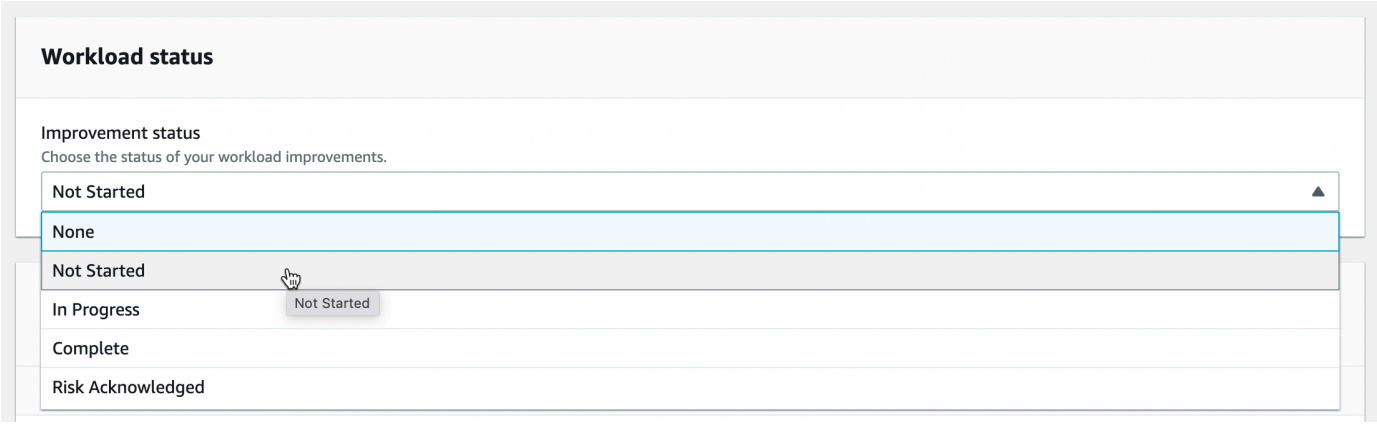
この特定のワークロード例では、 AWS Well-Architected Framework Lensによって3つの高リスク問題と1つの中リスクの問題が特定されました。



ワークロードの[改善ステータス]を更新して、ワークロードへの改善がまだ開始されていないことを周知します。

[改善ステータス] を変更するには:

1. 改善計画から、ページ上部のパンくずリストにあるワークロードの名前 (**Retail Website - North America**) をクリックします。
2. [プロパティ] タブをクリックします。
3. [ワークロードのステータス] セクションに移動し、ドロップダウンリストで [未開始] を選択します。



4. [概要] タブをクリックして [プロパティ] タブに戻り、[レンズ] セクションの AWS Well-Architected フレームワークリンクをクリックします。次に、ページ上部の [改善計画] タブをクリックします。

[Improvement items (改善項目)] セクションには、ワークロードで特定された推奨改善項目が表示されます。質問は、設定した優先度に基づいて並べ替えられ、まず高リスクの問題が、次に中リスクの問題が表示されます。

質問のベストプラクティスを表示するには、[Recommended improvement items (推奨改善項目)] を展開します。推奨改善アクションはそれぞれ、特定されたリスクを排除するか少なくとも軽減するのに役立つ、エキスパートからの詳細なガイダンスにリンクされています。

プロファイルがワークロードに関連付けられている場合は、優先度の高いリスクの数が [改善計画の概要] セクションに表示され、[プロファイルによる優先度] を選択することで [改善項目] のリストをフィルタできます。改善項目のリストには、[優先度] ラベルが表示されます。

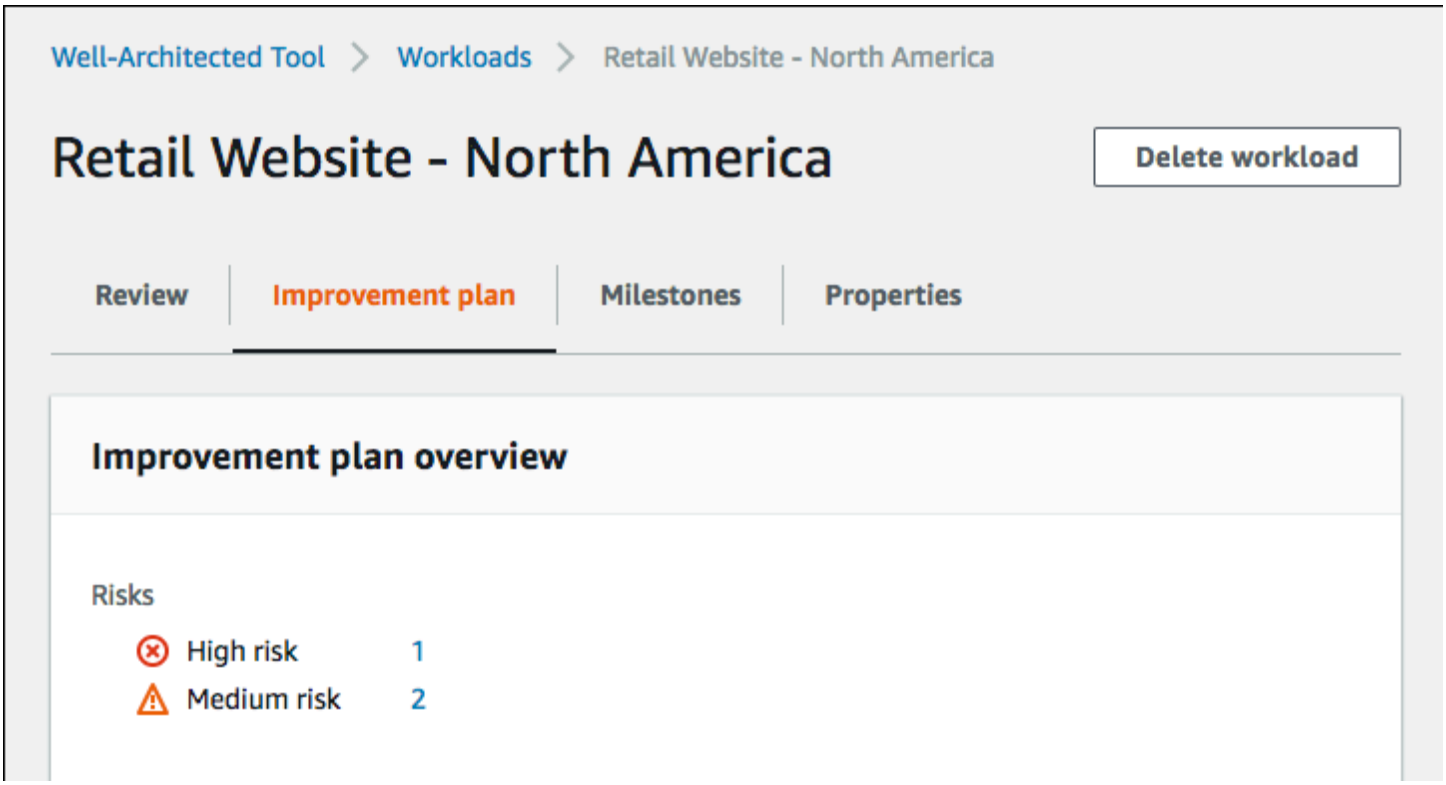
手順 4: 改善を行って進捗を評価する

この改善計画の一環として、リスクの高い問題の1つに、 CloudWatch AWS Auto Scaling Amazonとサポートをワークロードに追加することで対処しました。

[改善項目] セクションから:

1. 関連のある質問を選択し、変更を反映するように選択したベストプラクティスを更新します。改善点を記録するメモが追加されます。
2. 次に [保存して終了] を選択してワークロードの状態を更新します。

3. 変更を加えた後は [Improvement plan (改善計画)] に戻り、それらの変更がワークロードに与えた影響を確認できます。この例では、これらのアクションによりリスクプロファイルが改善され、高リスクの問題が 3 つから 1 つに減少しました。



この時点でマイルストーンを保存してから [Milestones (マイルストーン)] に移動し、ワークロードがどのように改善されたかを確認できます。

ワークロード

ワークロードとは、ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の集合のことです。

ワークロードは、1 つの AWS アカウント内のリソースのサブセットで構成されている場合もあれば、複数の AWS アカウントにまたがる複数のリソースの集合になっている場合もあります。中小企業では、ほんの数ワークロードになる一方、大企業では、数千ワークロードにもなることがあります。

左側のナビゲーションからアクセスできる [Workloads (ワークロード)] ページには、すべてのワークロードに関する情報と、共有されたワークロードが表示されます。

ワークロードごとに以下の情報が表示されます。

名前

ワークロードの名前。

所有者

ワークロードを所有する AWS アカウント ID。

回答された質問

回答された質問の数。

[High risks (高リスク)]

特定された高リスクの問題 (HRI) の数。

[Medium risks (中リスク)]

特定された中リスクの問題 (MRI) の数。

[Improvement status (改善ステータス)]

ワークロードに対して設定した改善ステータス。

- なし
- 未開始
- 進行中
- 完了
- Risk Acknowledged (リスク認識)

最終更新日

ワークロードが最後に更新された日時。

リストからワークロードを選択したら、次の操作を行います。

- ワークロードの詳細をレビューするには、[View details (詳細の表示)] を選択します。
- ワークロードのプロパティを変更するには、[Edit (編集)] を選択します。
- 他の AWS アカウント、ユーザー、AWS Organizations または組織部門 (OU) とのワークロード共有を管理するには、[詳細を表示]、[共有] の順に選択します。
- ワークロードとそのすべてのマイルストーンを削除するには、[Delete (削除)] を選択します。ワークロードの所有者のみがこれを削除できます。

> **Warning**
>
> 削除したワークロードを元に戻すことはできません。ワークロードに関連付けられているすべてのデータが削除されます。

高リスクの問題 (HRI) と中リスクの問題 (MRI)

AWS Well-Architected Tool で特定された 高リスクの問題 (HRI) は、ビジネスに重大な悪影響を及ぼす可能性があると AWS が認識した、アーキテクチャおよび運用上の選択肢です。HRI は、組織の運用、資産、個人に影響を及ぼす可能性があります。中リスクの問題 (MRI) もビジネスに悪影響を及ぼす可能性がありますが、その程度は比較的低くなります。これらの問題は、AWS Well-Architected Tool の回答に基づいています。対応するベストプラクティスは、AWS および AWS のお客様に広く適用されます。ここでのベストプラクティスとは、AWS Well-Architected フレームワークとレンズによって定義されるガイダンスです。

> **Note**
>
> これらはあくまでガイドラインであり、お客様はそのベストプラクティスを実践しないことでビジネスにどのような影響があるかを評価し、測定する必要があります。ワークロードにベストプラクティスを適用できない技術的またはビジネス上の具体的な理由がある場合、リスクは示された値よりも低くなる可能性があります。AWS では、お客様がこれらの理由とその理由によるベストプラクティスへの影響を、ワークロードのコメントに記録することをお勧めしています。特定されたすべての HRI と MRI の場合、AWS はお客様に対し、AWS

Well-Architected Tool で定義されているベストプラクティスを実践するようお勧めしています。ベストプラクティスを実装した場合は、AWS Well-Architected Tool でベストプラクティスが実装済みであるとマークして、問題が解決したことを示します。お客様がベストプラクティスを実装しないことを選択した場合、AWS は、実装しない理由と適切なビジネスレベルの承認を記録することをお勧めします。

ワークロードの定義

ワークロードを定義するには 2 つの方法があります。AWS WA Tool の [ワークロード] ページでは、テンプレートなしでワークロードを定義できます。または、[レビューテンプレート] ページでは、既存のレビューテンプレートを使用するか、新しいテンプレートを作成して、ワークロードを定義できます。

[ワークロード] ページでワークロードを定義するには

1. 左側のナビゲーションペインで [ワークロード] を選択します。
2. [ワークロードの定義] ドロップダウンを選択します。
3. [ワークロードの定義] を選択します。または、レビューテンプレートを作成していて、そこからワークロードを定義する場合は、[レビューテンプレートから定義] を選択します。
4. the section called “ワークロードの定義” の指示に従って、ワークロードプロパティを指定するか、任意でプロファイルとレンズを適用します。

[レビューテンプレート] ページからワークロードを定義するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. 既存のレビューテンプレートの名前を選択するか、the section called “レビューテンプレートの作成” の指示に従って新しいレビューテンプレートを作成します。
3. [テンプレートからワークロードを定義] を選択します。
4. the section called “テンプレートのワークロードを定義する” の指示に従って、レビューテンプレートからワークロードを作成します。

ワークロードの表示

自分が所有しているワークロードと、自分と共有されているワークロードの詳細を表示できます。

ワークロードを表示するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 以下のいずれかの方法で表示するワークロードを選択します。
   - ワークロードの名前を選択します。
   - ワークロードを選択したら、[詳細の表示] を選択します。

ワークロード詳細ページが表示されます。

> **Note**
>
> 必須フィールド [Review owner (レビューの所有者)] が追加されました。これにより、レビュープロセスの主担当者またはグループを簡単に識別できます。
> このフィールドが追加される前に定義されたワークロードを初めて表示すると、この変更が通知されます。[Edit (編集)] を選択して [Review owner (レビュー所有者)] フィールドを設定します。それ以上のアクションは必要ありません。
> [Acknowledge] (了解) を選択すると、[Review owner] (レビュー所有者) フィールドの設定が延期されます。その 60 日間、フィールドが空白であることを示すバナーが表示されます。バナーを削除するには、ワークロードを編集し、[Review owner (レビュー所有者)] を指定します。
> 指定された日付までにフィールドを設定しない場合、ワークロードへのアクセスが制限されます。ワークロードの表示と削除は続行できますが、[Review owner (レビュー所有者)] フィールドの設定以外は編集できません。ワークロードへの共有アクセスは、アクセスが制限されている間も影響を受けません。

ワークロードの編集

自分が所有しているワークロードの詳細を編集できます。

ワークロードを編集するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。

3. 編集するワークロードを選択したら、[Edit (編集)] を選択します。
4. ワークロードに変更を加えます。

   各フィールドの説明については、「ワークロードの定義」を参照してください。

   > **Note**
   >
   > 既存のワークロードを更新する場合、[Trusted Advisor をアクティブ化する] を使用できます。これにより、ワークロード所有者の IAM ロールが自動作成されます。Trusted Advisor が有効化されたワークロードに関連するアカウントの所有者は、IAM でロールを作成する必要があります。詳細については、「the section called “IAM でのアクティベーション Trusted Advisor ”」を参照してください。

5. [保存] を選択して、ワークロードに加えた変更を保存します。

   必須フィールドが空白の場合、または指定した値が無効な場合は、ワークロードに対する更新を保存する前に問題を修正する必要があります。

ワークロードの共有

自分が所有しているワークロードは、同じ AWS リージョン のその他 AWS アカウント、ユーザー、組織、および組織部門 (OU) と共有できます。

> **Note**
>
> ワークロードを共有できるのは、同じ AWS リージョン内だけです。
> ワークロードを他の AWS アカウント と共有する場合、受信者に `wellarchitected:UpdateShareInvitation` アクセス許可がないと、共有の招待を受け入れることはできません。アクセス許可ポリシーの例については、「the section called “へのアクセスの提供 AWS WA Tool”」を参照してください。

他の AWS アカウント やユーザーとワークロードを共有するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 次のいずれかの方法で、自分が所有しているワークロードを選択します。

- ワークロードの名前を選択します。
- ワークロードを選択したら、[詳細の表示] を選択します。

4. [共有] を選択します。次に、[作成]、[ユーザーまたはアカウントへの共有を作成] の順に選択し、ワークロードの招待状を作成します。
5. ワークロードを共有するユーザーの 12 桁の AWS アカウント ID または ARN を入力します。
6. 付与するアクセス許可を選択します。

   読み取り専用

   ワークロードへの読み取り専用アクセスを許可します。

   投稿者

   回答とそのメモへの更新アクセスと、残りのワークロードへの読み取り専用アクセスを許可します。
7. [作成] を選択して、指定した AWS アカウント またはユーザーにワークロードの招待を送信します。

ワークロードの招待が 7 日以内に承諾されない場合、招待は自動的に期限切れになります。

ユーザーとユーザーの AWS アカウント の両方にワークロードの招待がある場合、最高レベルのアクセス許可のワークロードの招待がユーザーに適用されます。

> **Important**
>
> ワークロードを組織または組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効にする必要があります。

ワークロードを組織や OU と共有するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 次のいずれかの方法で、自分が所有しているワークロードを選択します。
   - ワークロードの名前を選択します。
   - ワークロードを選択したら、[詳細を表示] を選択します。

4. [共有] を選択します。次に、[作成] と [Organizations への共有の作成] を選択します。
5. [ワークロード共有を作成] ページで、組織全体に許可を付与するのか、1 つ以上の OU に付与するのかを選択します。
6. 付与するアクセス許可を選択します。

   読み取り専用

   ワークロードへの読み取り専用アクセスを許可します。

   投稿者

   回答とそのメモへの更新アクセスと、残りのワークロードへの読み取り専用アクセスを許可します。
7. [作成] を選択してワークロードを共有します。

ワークロードへのアクセスを共有している人を確認するには、ワークロード詳細ページで [Shares] (共有) を選択します。

エンティティによるワークロードの共有を防止するため、`wellarchitected:CreateWorkloadShare` アクションを拒否するポリシーを追加します。

また、自分が所有しているカスタムレンズは、同じ AWS リージョン 内の他の AWS アカウント、ユーザー組織 OU と共有できます。詳細については、「カスタムレンズの共有」を参照してください。

共有についての検討事項

ワークロードは、最大 20 の異なる AWS アカウント およびユーザーと共有できます。ワークロードを共有できるのは、ワークロードと同じ AWS リージョンにあるアカウントとユーザーのみです。

2019 年 3 月 20 日以降に開設されたリージョンでワークロードを共有するには、自分と共有先の AWS アカウントの両方が AWS Management Console でそのリージョンを有効にする必要があります。詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

ワークロードは、AWS アカウント、アカウントの個々のユーザー、またはその両方と共有できます。ワークロードを AWS アカウント と共有すると、そのアカウントのすべてのユーザーにワークロードへのアクセスが付与されます。アカウントの特定のユーザーだけがアクセスを必要とする場合は、最小特権付与のベストプラクティスに従い、それらのユーザーと個別にワークロードを共有します。

AWS アカウント と、アカウントのユーザーの両方にワークロードの招待がある場合、最高レベルのアクセス許可が付与されているワークロード招待が、ワークロードへのユーザーのアクセス許可を判断します。ユーザーのワークロードの招待を削除した場合、ユーザーのアクセスは AWS アカウントのワークロードの招待によって決まります。ワークロードへのユーザーのアクセス権を削除するには、両方のワークロードの招待を削除します。

ワークロードを組織または 1 つ以上の組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効にする必要があります。

1 つの組織と 1 つ以上の OU の両方とワークロードを共有する場合、最高レベルのアクセス許可を持つワークロード招待によって、そのワークロードに対するアカウントのアクセス許可が決まります。

AWS Organizations 共有を有効にするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。
2. 左側のナビゲーションペインで [設定] を選択します。
3. [AWS Organizations のサポートを有効化] を選択します。
4. [設定を保存] を選択します。

共有アクセスの削除

ワークロードの招待は削除できます。ワークロードの招待を削除すると、ワークロードへの共有アクセスが削除されます。

ワークロードへの共有アクセスを削除するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 以下のいずれかの方法でワークロードを選択します。
   - ワークロードの名前を選択します。
   - ワークロードを選択したら、[詳細を表示] を選択します。
4. [共有] を選択します。
5. 削除するワークロードの招待を選択し、[削除] を選択します。
6. [Delete] を選択して確定します。

ユーザーとユーザーの AWS アカウント にワークロードの招待がある場合、ワークロードに対するユーザーのアクセス許可を削除するには、両方のワークロードの招待を削除する必要があります。

共有アクセスの変更

保留中または承諾されたワークロードの招待を変更できます。

ワークロードへの共有アクセスを変更するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 次のいずれかの方法で、自分が所有しているワークロードを選択します。
   - ワークロードの名前を選択します。
   - ワークロードを選択したら、[詳細を表示] を選択します。
4. [共有] を選択します。
5. 変更するワークロードの招待を選択し、[編集] を選択します。
6. AWS アカウント またはユーザーに付与する新しいアクセス許可を選択します。

   読み取り専用

   ワークロードへの読み取り専用アクセスを許可します。

   投稿者

   回答とそのメモへの更新アクセスと、残りのワークロードへの読み取り専用アクセスを許可します。
7. [保存] を選択します。

変更したワークロードの招待が 7 日以内に承諾されない場合は、自動的に期限切れになります。

ワークロードの招待の承諾と拒否

ワークロードの招待は、別の AWS アカウントが所有するワークロードを共有するためのリクエストです。ワークロードの招待を承諾すると、ワークロードが [ワークロード] ページと [ダッシュボード] ページに追加されます。ワークロードの招待を拒否すると、その招待はワークロードの招待リストから削除されます。

ワークロードの招待を承諾するまでに、7 日の猶予があります。7 日以内に招待を承諾しない場合は、自動的に期限切れになります。

> **Note**
>
> ワークロードは、同じ AWS リージョン内でのみ共有できます。

ワークロードの招待を承諾または拒否するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで、[Workload invitations (ワークロードの招待)] を選択します。
3. 承諾または拒否するワークロードの招待を選択します。
   - ワークロードの招待を承諾するには、[承諾] を選択します。

     ワークロードが [ワークロード] ページと [ダッシュボード] ページに追加されます。
   - ワークロードの招待を拒否するには、[拒否] を選択します。

     ワークロードの招待がリストから削除されます。

ワークロードの招待が承諾された後に共有アクセスを拒否するには、ワークロードのワークロード詳細ページで [Reject share] (共有を拒否) を選択します。

ワークロードの削除

不要になったワークロードは削除できます。ワークロードを削除すると、マイルストーンやワークロード共有の招待も含め、ワークロードに関連付けられているすべてのデータが削除されます。ワークロードを削除できるのは、ワークロードの所有者だけです。

> **Warning**
>
> 削除したワークロードを元に戻すことはできません。ワークロードに関連付けられているすべてのデータが完全に削除されます。

ワークロードを削除するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 削除するワークロードを選択したら、[Delete (削除)] を選択します。
4. [Delete (削除)] ウィンドウで、[Delete (削除)] を選択してワークロードとそのマイルストーンの削除を確認します。

エンティティによるワークロードの削除を防止するため、`wellarchitected:DeleteWorkload` アクションを拒否するポリシーを追加します。

ワークロードレポートの生成

レンズのワークロードレポートを生成できます。レポートには、ワークロードの質問への回答、コメント、特定された現在の中および高リスクの数が含まれています。質問で 1 つ以上のリスクが特定された場合、その質問のための改善計画により、それらのリスクを軽減するためのアクションが一覧表示されます。

ワークロードにプロファイルが関連付けられている場合は、プロファイルの概要情報と優先順位付けされたリスクがワークロードレポートに表示されます。

レポートを使用すると、AWS Well-Architected Tool にアクセスできない他のユーザーとワークロードに関する詳細を共有できます。

ワークロードレポートを生成するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 目的のワークロードを選択したら、[詳細を表示] を選択します。
4. レポートを生成するレンズを選択したら、[レポート生成] を選択します。

   レポートが生成され、そのダウンロードや表示が可能になります。

ワークロード詳細

ワークロード詳細ページには、マイルストーン、改善計画、ワークロード共有など、ワークロードに関する情報が表示されます。ページ上部のタブを使用して、さまざまな詳細セクションに移動します。

ワークロードを削除するには、[Delete workload (ワークロードの削除)] を選択します。ワークロードを削除できるのは、ワークロードの所有者だけです。

共有ワークロードへのアクセスを削除するには、[Reject share (共有の拒否)] を選択します。

トピック

[概要] タブ

初めてワークロードを表示したときには、まず [Overview (概要)] タブが表示されます。このタブには、ワークロードの全体的な状態、続いて各レンズの状態が表示されます。

すべての質問を完了していない場合は、ワークロードのドキュメント化を開始または続行するよう促すバナーが表示されます。

[Workload overview (ワークロードの概要)] セクションには、ワークロードの現在の全体的な状態と、[Workload notes (ワークロードコメント)] に入力したコメントが表示されます。状態またはコメントを更新するには、[Edit (編集)] を選択します。

ワークロードの現在の状態を記録するには、[Save milestone (マイルストーンの保存)] を選択します。マイルストーンは不変であり、保存後に変更することはできません。

ワークロードの状態の文書化を続けるには、[Start reviewing (レビューの開始)] を選択し、目的のレンズを選択します。

[Milestones] (マイルストーン) タブ

ワークロードのマイルストーンを表示するには、[Milestones (マイルストーン)] タブを選択します。

マイルストーンを選択したら、[レポートの生成] を選択して、マイルストーンに関連付けられたワークロードレポートを作成します。レポートには、ワークロードの質問への回答、コメント、マイルストーンが保存された時点での、ワークロードの中および高リスクの数が含まれています。

以下のいずれかの方法で、特定のマイルストーンの時点におけるワークロードの状態に関する詳細を表示できます。

- マイルストーンの名前を選択します。
- マイルストーンを選択したら、[View milestone (マイルストーンの表示)] を選択します。

[Properties] (プロパティ) タブ

ワークロードのプロパティを表示するには、[Properties (プロパティ)] タブを選択します。これらのプロパティの初期値は、ワークロードの定義時に指定された値です。[Edit (編集)] を選択して、変更を加えることができます。変更できるのは、ワークロードの所有者だけです。

プロパティの説明については、「ワークロードの定義」を参照してください。

[Shares] (共有) タブ

ワークロードの招待を表示または変更するには、[共有] タブを選択します。このタブは、ワークロードの所有者に対してのみ表示されます。

ワークロードへの共有アクセスを持つ各 AWS アカウント とユーザーごとに、次の情報が表示されます。

Principal

ワークロードへの共有アクセスを持つ AWS アカウント ID またはユーザー ARN。

ステータス

ワークロード招待のステータス。

- [保留中]

  招待は承諾または拒否待ちです。ワークロードの招待が 7 日以内に承諾されない場合は、自動的に期限切れになります。

- 承諾

  招待は承諾されました。

- 拒否

  招待は拒否されました。

- 失効済み

  招待は 7 日以内に承諾または拒否されませんでした。

アクセス許可

AWS アカウント またはユーザーに付与されるアクセス許可。

- 読み取り専用

  プリンシパルは、ワークロードに対する読み取り専用アクセス権を持ちます。

- 投稿者

  プリンシパルは回答とそのメモを更新でき、残りのワークロードへの読み取り専用アクセス権を持ちます。

アクセス許可の詳細

アクセス許可の詳細説明。

同じ AWS リージョン 内の別の AWS アカウント またはユーザーとワークロードを共有するには、[作成] を選択します。ワークロードは、最大 20 の異なる AWS アカウント およびユーザーと共有できます。

ワークロードの招待を削除するには、招待を選択して [削除] を選択します。

ワークロードの招待を変更するには、招待を選択し、[編集] を選択します。

レンズ

レンズは、ベストプラクティスに照らしてアーキテクチャを評価し、改善すべき分野を特定する一貫した方法を提供します。ワークロードが定義されると、AWS Well-Architected フレームワークレンズが自動適用されます。

ワークロードには、1 つまたは複数のレンズを適用できます。各レンズには、それぞれ独自の質問、ベストプラクティス、コメント、改善計画があります。

ワークロードに適用できるレンズには、[レンズカタログ] と [カスタムレンズ] の 2 種類があります。

- レンズカタログ:によって作成および管理されている公式レンズ AWS。レンズカタログはすべてのユーザーが利用でき、追加でインストールしなくても使用できます。
- カスタムレンズ: AWS 公式コンテンツではないユーザー定義レンズ。独自の柱、質問、ベストプラクティス、改善計画を使用して、カスタムレンズを作成したり、他の AWS アカウントとカスタムレンズを共有したりできます。

一度に 5 つのレンズをワークロードに追加でき、1 つのワークロードには最大 20 のレンズを適用できます。

ワークロードからレンズを削除すると、レンズに関連付けられたデータが保持されます。ワークロードにレンズを追加し直した場合、データが復元されます。

ワークロードへのレンズの追加

ワークロードにレンズを追加するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 目的のワークロードを選択したら、[詳細を表示] を選択します。
4. 追加するレンズを選択し、[保存] を選択します。

   レンズは、[カスタムレンズ]、[レンズカタログ]、またはその両方から選択できます。

ワークロードには最大 20 個のレンズを追加できます。

AWS レンズカタログの詳細については、AWS Well-Architected Lensesをご覧ください。すべてのレンズのホワイトペーパーがレンズカタログにレンズとして提供されているわけではありません。

> **免責事項**
>
> AWS 他のユーザーまたはアカウントが作成したカスタムレンズにアクセスしたり適用したりすることで、他のユーザーが作成して共有したカスタムレンズが顧客契約で定義されている第三者コンテンツであることを認めたものとみなされます。 AWS

ワークロードからのレンズの削除

ワークロードからレンズを削除するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 目的のワークロードを選択したら、[詳細を表示] を選択します。
4. 削除するレンズを選択解除し、[Save] (保存) を選択します。

   AWS Well-Architected Framework Lensはワークロードから削除できません。

レンズに関連するデータは保持されます。レンズをワークロードに戻すと、データが復元されます。

レンズの詳細

レンズの詳細を表示するには、レンズを選択します。

[概要] タブ

[Overview (概要)] タブには、回答された質問の数など、レンズに関する一般的な情報が表示されます。このタブから続けて、ワークロードの確認、レポートの生成、レンズメモの編集を行うことができます。

[Improvement Plan] (改善計画) タブ

[Improvement Plan (改善計画)] タブには、ワークロードを改善するために推奨されるアクションのリストが表示されます。リスクと柱に基づいて推奨事項をフィルタ処理できます。

[Shares] (共有) タブ

カスタムレンズの場合、[Shares] (共有) タブには、そのレンズが共有されている IAM プリンシパルのリストが表示されます。

カスタムレンズ

独自の柱、質問、ベストプラクティス、改善計画を使用して、カスタムレンズを作成できます。AWS が提供するレンズと同じように、カスタムレンズをワークロードに適用します。また、自分が作成したカスタムレンズを他の AWS アカウントと共有したり、他の人が所有するカスタムレンズを自分と共有したりできます。

カスタムレンズの質問は、特定のテクノロジーに特化したり、組織内のガバナンスニーズに対応したり、Well-Architected フレームワークや AWS レンズで提供されるガイダンスを拡張したりできるようにカスタマイズできます。既存のレンズと同様に、マイルストーンを作成して経時的な進行状況を追跡し、レポートを生成して定期的なステータスを提供できます。

トピック

- カスタムレンズの表示
- カスタムレンズの作成
- カスタムレンズのプレビュー
- カスタムレンズの最初の公開
- カスタムレンズの更新の公開
- カスタムレンズの共有
- カスタムレンズにタグを追加する
- カスタムレンズの削除
- レンズ形式の仕様

カスタムレンズの表示

自分が所有しているカスタムレンズと、自分と共有されているカスタムレンズの詳細を表示できます。

レンズを表示するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左側のナビゲーションペインで [カスタムレンズ] を選択します。

> **Note**
>
> カスタムレンズを作成していない場合や、カスタムレンズを共有していない場合、[カスタムレンズ] セクションには何も表示されません。

3. 表示するカスタムレンズを選択します。
   - [Owned by me] (自分が所有) – 自分が作成したカスタムレンズを表示します。
   - [Shared with me] (自分と共有) – 自分と共有されているカスタムレンズを表示します。
4. 以下のいずれかの方法で、表示するカスタムレンズを選択します。
   - レンズの名前を選択します。
   - レンズを選択したら、[View details] (詳細の表示) を選択します。

[レンズの詳細] ページが表示されます。

[Custom lenses] (カスタムレンズ) ページには以下のフィールドがあります。

名前

レンズの名前。

[所有者]

カスタムレンズを所有している AWS アカウント ID。

ステータス

[PUBLISHED] (公開済み) というステータスは、カスタムレンズが公開済みで、ワークロードに適用したり他の AWS アカウントと共有したりできることを意味します。

[DRAFT] (下書き) のステータスは、カスタムレンズが作成されたものの、まだ公開されていないことを意味します。カスタムレンズは、ワークロードに適用または共有する前に、公開する必要があります。

バージョン

カスタムレンズのバージョン名。

最終更新日

カスタムレンズが最後に更新された日時。

カスタムレンズの作成

カスタムレンズを作成するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. [Create custom lens] (カスタムレンズの作成) を選択します。
4. JSON テンプレートファイルをダウンロードするには、[Download file] (ファイルのダウンロード) を選択します。
5. 任意のテキストエディタで JSON テンプレートファイルを開き、カスタムレンズのデータを追加します。このデータには、柱、質問、ベストプラクティス、改善計画リンクが含まれます。

   詳細については、「レンズ形式の仕様」を参照してください。カスタムレンズのサイズは 500 KB を超えることはできません。
6. [ファイルを選択] を選択し、JSON ファイルを選択します。
7. (オプション) [タグ] セクションで、ワークロードレンズに関連付けるタグを追加します。
8. [送信とプレビュー] を選択してカスタムレンズをプレビューするか[送信] を選択して、プレビューせずにカスタムレンズを送信します。

   [送信とプレビュー] を選択してカスタムレンズをプレビューして送信する場合は、[次へ] を選択すると、レンズのプレビューに移動できます。[プレビューの終了] を選択すると、[カスタムレンズ] に戻れます。

検証に失敗した場合は、JSON ファイルを編集して、カスタムレンズを再度作成してみてください。

JSON AWS WA Tool ファイルを検証すると、カスタムレンズが [カスタムレンズ] に表示されます。

カスタムレンズが作成されると、[DRAFT](下書き) ステータスになります。レンズをワークロードに適用したり他の AWS アカウントと共有したりするには、レンズを公開する必要があります。

AWS アカウントでは 最大 15 個のカスタムレンズを作成できます。

> **免責事項**
>
> カスタムレンズにエンドユーザーまたはその他の個人を特定できる情報 (PII) を含めたり、カスタムレンズを介してこれらを収集したりしないでください。自分のカスタムレンズ、または自分のアカウントで使用している共有されたカスタムレンズに PII が含まれる、またはこれらを介して PII が収集される場合、お客様は、含まれる PII が適用法に従って処理されること、適切なプライバシー通知を行うこと、および当該データを処理するために必要な同意を得ることに責任を負います。

カスタムレンズのプレビュー

カスタムレンズをプレビューするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [カスタムレンズ] を選択します。
3. プレビューできるのは [下書き] ステータスのレンズだけです。目的の [下書き] カスタムレンズ、[プレビューエクスペリエンス] の順に選択します。
4. [次へ] を選択して、レンズのプレビューを確認します。
5. (オプション) プレビューの各質問内のベストプラクティスを選択し、[回答に基づいて更新する] を選択してリスクロジックをテストすることで、[改善計画] を確認できます。変更が必要な場合は、公開前に JSON テンプレート内の [リスクルール] を更新します。
6. [プレビューを終了] を選択してカスタムレンズに戻ります。

> **Note**
>
> カスタムレンズの作成時に、[送信とプレビュー] を選択しても、カスタムレンズをプレビューできます。

カスタムレンズの最初の公開

カスタムレンズを公開するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. 目的のカスタムレンズを選択し、[Publish lens] (レンズを公開) を選択します。
4. [Version name] (バージョン名) ボックスに、バージョン変更のための一意の識別子を入力します。この値は最大 32 文字で、英数字とピリオド (「.」) のみを使用できます。
5. [Publish custom lens] (カスタムレンズを公開) を選択します。

   カスタムレンズが発行されると、[発行済み] ステータスになります。

これで、カスタムレンズをワークロードに適用したり、他の AWS アカウント またはユーザーを共有できるようになります。

カスタムレンズの更新の公開

既存のカスタムレンズの更新を公開するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. 目的のカスタムレンズを選択し、[Edit] (編集) を選択します。
4. 更新された JSON ファイルの準備ができていない場合は、[Download file] (ファイルをダウンロード) を選択して、現在のカスタムレンズのコピーをダウンロードします。ダウンロードした JSON ファイルを任意のテキストエディタで編集し、必要な変更を加えます。
5. [ファイルを選択] を選択して更新された JSON ファイルし、[送信とプレビュー] を選択してカスタムレンズをプレビューするか、[送信] を選択して、プレビューせずにカスタムレンズを送信します。

   カスタムレンズのサイズは 500 KB を超えることはできません。

   JSON AWS WA Tool ファイルを検証すると、カスタムレンズは「ドラフトステータス」の「カスタムレンズ」に表示されます。

6. 再度カスタムレンズを選択し、[Publish lens] (レンズを公開) を選択します。
7. [Review changes before publish] (公開前に変更内容を確認) を選択すると、カスタムレンズに加えた変更が正しいかどうかを確認できます。これには、次の確認が含まれます。

   - カスタムレンズの名前
   - 柱の名前
   - 新規作成、更新、削除された質問

   [次へ] をクリックします。
8. バージョン変更の種類を指定します。

   メジャーバージョン

   レンズに大きな変更が加えられたことを示します。カスタムレンズの意味に影響を与える変更に使用します。

   レンズが適用されたワークロードには、カスタムレンズの新しいバージョンが利用可能であることが通知されます。

   バージョンの大きな変更は、レンズを使用しているワークロードには自動的に適用されません。

   マイナーバージョン

   レンズに小さな変更が加えられたことを示します。テキストの変更や URL リンクの更新など、小さな変更に使用します。

   バージョンの小さな変更は、カスタムレンズを使用しているワークロードに自動的に適用されます。

   [次へ] をクリックします。
9. [Version name] (バージョン名) ボックスに、バージョン変更のための一意の識別子を入力します。この値は最大 32 文字で、英数字とピリオド (「.」) のみを使用できます。
10. [Publish custom lens] (カスタムレンズを公開) を選択します。

    カスタムレンズが発行されると、[発行済み] ステータスになります。

これで、更新されたカスタムレンズをワークロードに適用したり、他の AWS アカウント やユーザーと共有したりできます。

更新がバージョンの大きな変更である場合、旧バージョンのレンズが適用されているワークロードには、新しいバージョンが利用可能であることが通知され、アップグレードのオプションが提示されます。

バージョンの小さな更新は、通知なしで自動的に適用されます。

カスタムレンズのバージョンは、最大 100 バージョンまで作成できます。

カスタムレンズの共有

カスタムレンズは AWS アカウント、他のユーザー AWS Organizations、および組織単位 (OU) と共有できます。

AWS アカウント カスタムレンズを他のユーザーと共有するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool のコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. 共有するカスタムレンズを選択したら、[View details] (詳細の表示) を選択します。
4. [レンズの詳細] ページで、[共有] を選択します。次に、[作成]、[ユーザーまたはアカウントへの共有を作成] の順に選択し、レンズ共有の招待を作成します。
5. カスタムレンズを共有したいユーザーの 12 桁の AWS アカウント ID または ARN を入力します。
6. [作成] を選択して、 AWS アカウント 指定したユーザーまたはユーザーにレンズ共有の招待状を送信します。

カスタムレンズは最大 300 AWS アカウント 人またはユーザーと共有できます。

レンズ共有の招待が 7 日以内に承諾されない場合、招待は自動的に期限切れになります。

> **Important**
>
> カスタムレンズを組織または組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効化する必要があります。

カスタムレンズを組織または OU と共有するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左側のナビゲーションペインで [カスタムレンズ] を選択します。
3. 共有するカスタムレンズを選択します。
4. [レンズの詳細] ページで、[共有] を選択します。次に、[作成] と [Organizations への共有の作成] を選択します。
5. [カスタムレンズ共有を作成] ページで、アクセス許可を組織全体に付与するのか、1 つ以上の OU に付与するのかを選択します。
6. [作成] を選択してカスタムレンズを共有します。

カスタムレンズへの共有アクセスを持つ人を確認するには、レンズの詳細ページで [Shares] (共有) を選択します。

> **免責事項**
>
> カスタムレンズを他のユーザーと共有することで AWS アカウント、 AWS そのカスタムレンズを他のアカウントでも利用できるようになることに同意したものとみなされます。他のアカウントは、お客様がご自身のカスタムレンズを削除したり、 AWS アカウント お客様のカスタムレンズを終了したりしても、共有しているカスタムレンズに引き続きアクセスし、使用することができます。 AWS アカウント

カスタムレンズにタグを追加する

カスタムレンズにタグを追加するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左側のナビゲーションペインで [カスタムレンズ] を選択します。
3. 更新するカスタムレンズを選択します。
4. [タグ] セクションで、[タグを管理] を選択します。
5. [新しいタグの追加] を選択し、追加する各タグに[キー] および [値] を入力します。
6. [保存] を選択します。

タグを削除するには、削除するタグの横にある[削除] を選択します。

カスタムレンズの削除

カスタムレンズを削除するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ AWS Well-Architected Tool でコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. 削除するカスタムレンズを選択したら、[Delete] (削除) を選択します。
4. [削除] を選択します。

   レンズが適用された既存のワークロードには、カスタムレンズが削除されたことが通知されますが、引き続き使用できます。新しいワークロードにカスタムレンズを適用できなくなりました。

> **免責事項**
>
> カスタムレンズを他のユーザーと共有することで AWS アカウント、 AWS そのカスタムレンズを他のアカウントでも利用できるようになることに同意したものとみなされます。他のアカウントは、お客様がご自身のカスタムレンズを削除したり、 AWS アカウント お客様のカスタムレンズを終了したりしても、共有しているカスタムレンズに引き続きアクセスし、使用することができます。 AWS アカウント

レンズ形式の仕様

レンズは特定の JSON 形式を使用して定義されます。カスタムレンズの作成を開始する際に、テンプレートの JSON ファイルをダウンロードするオプションがあります。このファイルで柱、質問、ベストプラクティス、および改善計画の基本構造を定義するため、これをカスタムレンズの基礎として使用できます。

[Lens] (レンズ) セクション

このセクションでは、カスタムレンズ自体の属性を定義します。これには、名前と説明が含まれます。

- `schemaVersion`: 使用するカスタムレンズスキーマのバージョン。テンプレートによって設定されます。変更しないでください。

- name: レンズの名前。名前は最大 128 文字です。
- description: レンズの説明文。このテキストは、ワークロードの作成時に追加するレンズを選択するとき、または後で既存のワークロードに適用するレンズを選択するときに表示されます。説明は最大 2,048 文字です。

```
   "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.",
```

[Pillars] (柱) セクション

このセクションでは、カスタムレンズに関連する柱を定義します。 AWS 質問をWell-Architected Frameworkの柱にマッピングすることも、独自の柱を定義することも、あるいはその両方を行うこともできます。

カスタムレンズには最大 10 の柱を定義できます。

- id: 柱の ID。ID は 3 ~ 128 文字で、英数字とアンダースコア (「_」) のみ使用できます。柱に使用される ID は一意である必要があります。

  質問をフレームワークの柱にマッピングするときは、次の ID を使用します。

  - operationalExcellence
  - security
  - reliability
  - performance
  - costOptimization
  - sustainability
- name: 柱の名前。名前は最大 128 文字です。

```
    "pillars": [
       {
           "id": "company_Privacy",
           "name": "Privacy Excellence",
           .
```

```
            .
            .
        },
        {
            "id": "company_Security",
            "name": "Security",
            .
            .
            .
        }
    ]
```

[Questions] (質問) セクション

このセクションでは、柱に関連する質問を定義します。

カスタムレンズの柱には最大 20 の質問を定義できます。

- id: 質問の ID。ID は 3 ~ 128 文字で、英数字とアンダースコア (「_」) のみ使用できます。質問に使用される ID は一意である必要があります。
- title: 質問のタイトル。タイトルは最大 128 文字です。
- description: 質問について詳しく説明します。説明は最大 2,048 文字です。
- helpfulResource displayText: オプション。質問に関する有用な情報を提供するテキスト。テキストは最大 2,048 文字です。helpfulResource url を指定する場合は必ず指定します。
- helpfulResource url: オプション。質問をより詳細に説明する URL リソース。URL は、http:// または https:// で始まる必要があります。

> **Note**
>
> カスタムレンズワークロードを Jira に同期すると、質問には質問の「ID」と「タイトル」の両方が表示されます。
> Jira チケットで使用される形式はです。[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"
        },
        .
        .
        .
    }
]
```

[Choice] (選択肢) セクション

このセクションでは、質問に関連付けられている選択肢を定義します。

カスタムレンズの質問には最大 15 の選択肢を定義できます。

- id: 選択肢の ID。ID は 3 ~ 128 文字で、英数字とアンダースコア (「_」) のみ使用できます。質問の選択肢ごとに固有の ID を指定する必要があります。サフィックスが _no の選択肢を追加すると、質問では None of these の選択肢として扱われます。
- title: 選択肢のタイトル。タイトルは最大 128 文字です。
- helpfulResource displayText: オプション。選択肢に関する有用な情報を提供するテキスト。テキストは最大 2,048 文字です。helpfulResource url を指定する場合は必ず含めます。
- helpfulResource url: オプション。選択肢をより詳細に説明する URL リソース。URL は、http:// または https:// で始まる必要があります。

- improvementPlan displayText: 選択肢の改善方法を説明するテキスト。テキストは最大 2,048 文字です。None of these の選択肢を除き、各選択肢には improvementPlan が必要です。
- improvementPlan url: オプション。改善に役立つ URL リソース。URL は、http:// または https:// で始まる必要があります。
- additionalResources type: オプション。追加リソースのタイプ。この値は HELPFUL_RESOURCE または IMPROVEMENT_PLAN となります。
- additionalResources content: オプション。追加リソースに対して、displayText および url の値を指定します。選択肢には、役立つ追加リソースを最大 5 つと、追加の改善計画項目を 5 つまで指定できます。
  - displayText: オプション。役に立つリソースまたは改善計画を説明するテキスト。テキストは最大 2,048 文字です。url を指定する場合は必ず含めます。
  - url: オプション。役に立つリソースや改善計画の URL リソース。URL は、http:// または https:// で始まる必要があります。

> **Note**
>
> カスタムレンズワークロードを Jira に同期すると、選択肢には質問と選択肢の「ID」と、選択肢の「タイトル」が表示されます。
> 使用される形式はです。[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"
              }

            }
```

[Risk Rules] (リスクルール) セクション

このセクションでは、選択した選択肢がリスクレベルを決定する方法を定義します。

質問ごとに最大 3 つのリスクルールを定義できます (リスクレベルごとに 1 つ)。

- `condition`: 質問のリスクレベルに対応する選択肢のブール式、または `default`。

  各質問には、`default` リスクルールが必要です。
- `risk`: 条件に関連するリスクを示します。有効な値は、`HIGH_RISK`、`MEDIUM_RISK`、`NO_RISK` です。

リスクルールの順序は重要です。`true` に評価された最初の `condition` によって、その質問のリスクが設定されます。リスクルールを実装する一般的なパターンは、まずリスクが最も低い (そして一般的に最も詳細な) ルールから実装し、最後にリスクが最も高い (および最も限定的でない) ルールを実装することです。

例:

```
"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"
      }
]
```

質問に 3 つの選択肢がある場合 (choice_1、choice_2、choice_3) の場合、これらのリスクルールは次のように動作します。

- 3 つの選択肢がすべて選択されている場合、リスクなし。
- choice_1 または choice_2 のいずれかが選択され、かつ choice_3 が選択された場合、中リスク。
- choice_1 が選択されず、choice_3 が選択された場合も中リスクとなります。
- 上記の条件のいずれにも当てはまらない場合、高リスク。

レンズのアップグレード

AWS AWS が提供するWell-Architected Framework Lensやその他のレンズは、新しいサービスの導入、クラウドベースのシステムの既存のベストプラクティスの改良、新しいベストプラクティスの追加に応じて更新されます。 AWS WA Tool レンズの新しいバージョンがリリースされると、最新のベストプラクティスを反映するようにアップグレードされます。定義された新しいワークロードでは、新しいバージョンのレンズが使用されます。

レンズは、ワークロードに適用したカスタムレンズまたは、レビューテンプレートに新しいメジャーなバージョンが公開された場合にも、アップグレードされます。

レンズのアップグレードは、以下のいずれかの組み合わせで構成されます。

- 新しい質問やベストプラクティスの追加
- 推奨されなくなった古い質問やプラクティスの削除
- 既存の質問またはベストプラクティスの更新
- 柱の追加または削除

既存の質問に対する回答は保持されます。

> **Note**
>
> レンズアップグレードを元に戻すことはできません。ワークロードを最新のレンズバージョンにアップグレードした後に、以前のバージョンのレンズに戻ることはできません。

レンズのアップグレードの選択

[通知] ページには、最新のレンズバージョンが使用されていない各ワークロードの情報が表示されます。

ワークロードごとに以下の情報が表示されます。

リソース

ワークロードまたはレビューテンプレートの名前。

リソースタイプ

リソースのタイプ。これはワークロードまたはレビューテンプレートのいずれかとなります。

関連付けられたリソース

レンズの名前。

[通知タイプ]

アップグレード通知のタイプ。

- [Not current (最新でない)] - ワークロードには、最新でなくなったバージョンのレンズが使用されています。改良されたガイダンスを表示するには、最新バージョンのレンズにアップグレードしてください。
- [Deprecated] (廃止) - ワークロードには、ベストプラクティスを反映しなくなったバージョンのレンズが使用されています。最新バージョンのレンズにアップグレードします。
- [Deleted] (削除) - ワークロードは、所有者によって削除されたレンズを使用しています。

[Version in use] (使用中のバージョン)

ワークロードに現在使用されているレンズのバージョン。

[Current available version (現在使用可能なバージョン)]

アップグレード可能なレンズのバージョン。レンズが削除されている場合は [None] (なし) と表示されます。

ワークロードに関連付けられているレンズをアップグレードするには、ワークロード名を選択しから、[Upgrade lens version (レンズのバージョンのアップグレード)] を選択します。

レンズのアップグレード

レンズはワークロードとレビューテンプレートに合わせてアップグレードできます。

> **Note**
>
> レンズアップグレードを元に戻すことはできません。ワークロードまたはレビューテンプレートを最新のレンズバージョンにアップグレードした後は、レンズの前のバージョンに戻すことはできません。

ワークロード用のレンズのアップグレード

1. [通知] ページで、アップグレードするワークロードを選択し、[レンズバージョンをアップグレード] を選択します。各柱の変更内容に関する情報が表示されます。

   > **Note**
   >
   > ワークロードの [概要] タブから [利用可能なアップグレードを表示] を選択することもできます。

2. ワークロードのレンズをアップグレードする前に、今後の参照用に既存のワークロードの状態を保存するためのマイルストーンが作成されます。マイルストーンの一意の名前を [マイルストーン名] フィールドに入力します。
3. [これらの変更を理解し、受け入れます] の横にある [確認] ボックスを選択し、[保存] を選択します。

レンズをアップグレードすると、[マイルストーン] タブで以前のバージョンのレンズを表示できます。

レビューテンプレート用のレンズのアップグレード

1. レビューテンプレート用にレンズをアップグレードするには、以下を選択します。
2. [通知] ページで、アップグレードするレビューテンプレートを選択し、[レンズバージョンをアップグレード] を選択します。各柱の変更内容に関する情報が表示されます。

   > **Note**
   >
   > レビューテンプレートの [概要] タブから [利用可能なアップグレードを表示] を選択することもできます。

3. [これらの変更を理解し、受け入れます] の横にある [確認] ボックスを選択し、[アップグレードしてテンプレートの回答を編集] を選択してレビューテンプレートのベストプラクティスの質問への回答を調整するか、[アップグレード] を選択してテンプレートの回答を調整せずにレンズをアップグレードします。

レンズカタログ

レンズカタログは、 up-to-date テクノロジーと業界に焦点を当てたベストプラクティスを提供する、 AWS AWS WA Tool 公式に作成されたレンズのコレクションです。これらのレンズはすべてのユーザーが利用でき、追加でインストールしなくても使用できます。

以下の表は、 AWS 現在レンズカタログで入手可能なすべての公式レンズをまとめたものです。

名前	説明
AWS Well-Architected フレームワーク	デフォルトですべてのワークロードに適用されます。信頼性、セキュリティ、効率、コスト効果が高く、持続可能なシステムを設計し、クラウド内で運用するためのアーキテクチャのベストプラクティスのコレクションです。
コネクテッド・モビリティ	交通システムにテクノロジーを組み込み、全体的なモビリティ体験を向上させるためのベストプラクティス。
コンテナビルド	コンテナの設計と構築プロセスに関するベストプラクティスを提供します。

名前	説明
データ分析	AWS 実際のケーススタディから収集された洞察が含まれており、Well-Architected 分析ワークロードの主要な設計要素と、改善のための推奨事項を学ぶのに役立ちます。
DevOps	あらゆる規模の組織が、最新のテクノロジーとベストプラクティスを活用して大きなビジネス価値をもたらすことができる、迅速でセキュリティ重視の文化を育むために採用できる、構造化されたアプローチについて説明します。DevOps
政府	AWS政府サービスの設計と提供に関するベストプラクティス
ヘルスケア業界	AWS クラウドでのヘルスケアワークロードの設計、デプロイ、管理方法に関するベストプラクティスとガイダンスです。
IoT	AWSでモノのインターネット (IoT) ワークロードを管理するためのベストプラクティス
M&A、価値の創造	プライベートエクイティの合併や買収活動など、企業の成長を促進する方法を模索する際に考慮すべき追加の質問をいくつか挙げています。
機械学習	でのMachine Learning リソースとワークロードの管理に関するベストプラクティス AWS
移行	への移行方法に関するベストプラクティス AWS クラウド
SaaS	AWS クラウドでの Software as a Service (SaaS) ワークロードの設計、デプロイ、構築に焦点を当てています。

名前	説明
SAP	の SAP ワークロードの設計原則とベストプラクティス AWS クラウド
サーバーレスアプリケーション	上にサーバーレスワークロードを構築するためのベストプラクティス。 AWS RESTful マイクロサービス、モバイルアプリケーションバックエンド、ストリーム処理、ウェブアプリケーションなどのシナリオについて取り上げます。

レビューテンプレート

Well-Architected フレームワークとカスタムレンズのベストプラクティスに関する質問への回答があらかじめ入力された AWS WA Tool でレビューテンプレートを作成できます。Well-Architected レビューテンプレートがあれば、Well-Architected レビューを実施する際に、複数のワークロードに共通するベストプラクティスについて同じ回答を手動で入力する必要がなくなり、チームやワークロード全体でベストプラクティスの一貫性と標準化を促進できます。

レビューテンプレートを作成すると、ベストプラクティスに関する一般的な質問に回答したり、メモを作成したりできます。メモは、別の IAM ユーザーやアカウント、あるいは同じ AWS リージョン内の組織や組織部門と共有できます。レビューテンプレートからワークロードを定義できます。これにより、一般的なベストプラクティスを拡張し、ワークロード全体の冗長性を減らすことができます。

レビューテンプレートの作成

レビューテンプレートを作成するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. [テンプレートを作成] をクリックします。
3. [テンプレートの詳細を指定] ページで、レビューテンプレートの [名前] と [説明] を入力します。
4. (オプション) [テンプレートノート] セクションと [タグ] セクションに、レビューテンプレートに関連付けるテンプレートノートまたはタグを追加します。追加したメモはレビューテンプレートを使用するすべてのワークロードに適用されますが、タグはレビューテンプレートに固有のものです。

   タグの詳細については、「AWS WA Tool リソースのタグ付け」を参照してください。
5. [次へ] を選択します。
6. [レンズを適用] ページで、レビューテンプレートに適用するレンズを選択します。適用できるレンズの数は最大 20 です。

   レンズは、[カスタムレンズ]、[レンズカタログ]、またはその両方から選択できます。

> **Note**
>
> 共有されているレンズはレビューテンプレートには適用できません。

7. [テンプレートを作成] をクリックします。

作成したレビューテンプレートに関する質疑応答を始めるには

1. テンプレートの [概要] タブの [質問への回答を開始] 情報アラートにある、[質問に答える] ドロップダウンでレンズを選択します。

> **Note**
>
> [レンズ] セクションに移動してレンズを選択し、[質問に答える] を選択することもできます。

2. レビューテンプレートに適用した各レンズについて、該当する質問に答え、完了したら [保存して終了] を選択します。

レビューテンプレートを作成したら、そのテンプレートから新しいワークロードを定義できます。

レビューテンプレートの [概要] タブには、[テンプレートの詳細] セクションで回答された質問の合計数と、[レンズ] セクションの各レンズについて回答された質問の数が反映されます。

レビューテンプレートの編集

レビューテンプレートを編集するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. 編集するレビューテンプレートの名前を選択します。
3. レビューテンプレートの [名前]、[説明]、または [テンプレートノート] を更新するには、[概要] タブの [テンプレートの詳細] セクションで [編集] を選択します。
   a. [名前]、[説明]、または [テンプレートノート] を変更します。
   b. [テンプレートを保存] を選択し、変更内容を反映してレビューテンプレートを更新します。
4. レビューテンプレートに適用するレンズを更新するには、[概要] タブの [レンズ] セクションで、[適用したレンズを編集] を選択します。

a. 追加または削除するレンズのチェックボックスをオンまたはオフにします。

レンズは、[カスタムレンズ]、[レンズカタログ]、またはその両方から選択あるいは選択解除できます。

b. [テンプレートを保存] を選択し、変更を保存します。

5. レンズに関するベストプラクティスの質問への回答を更新するには、[概要] タブの [レンズ] セクションでレンズの名前を選択します。

a. [レンズの概要] セクションで、[質問に答える] を選択します。

> **Note**
>
> オプションで、左側のナビゲーションペインにある [レビューテンプレート] ドロップダウンでレンズの名前を選択すると、[レンズの概要] セクションに移動できます。

b. 変更するベストプラクティスの回答の横にあるチェックボックスをオンまたはオフにします。

c. [保存] を選択して、変更を保存して適用します。

レビューテンプレートの共有

レビューテンプレートは、ユーザーやアカウントと共有することも、組織全体または組織部門と共有することもできます。

レビューテンプレートを共有するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. 共有するレビューテンプレートの名前を選択します。
3. [共有] タブを選択します。
4. ユーザーまたはアカウントと共有するには、[作成] を選択し、[IAM ユーザーまたはアカウントと共有] を選択します。[招待を送信] ボックスで、ユーザー ID またはアカウント ID を指定し、[作成] を選択します。
5. 組織または組織部門と共有するには、[作成] を選択し、[Organizations と共有] を選択します。組織全体で共有するには、[組織全体に許可を付与] を選択します。組織部門と共有するには、[個々の組織部門に許可を付与] を選択し、ボックスで組織部門を指定して [作成] を選択します。

> **Important**
>
> プロファイルを組織または組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効にする必要があります。

テンプレートのワークロードを定義する

作成したレビューテンプレートまたは共有されているレビューテンプレートからワークロードを定義できます。削除されたレビューテンプレートから新しいワークロードを定義することはできません。レビューテンプレートに古いバージョンのレンズが含まれている場合は、レビューテンプレートをアップグレードしてから新しいワークロードを定義する必要があります。レビューテンプレートのアップグレード方法の詳細については、「the section called “レンズのアップグレード”」を参照してください。

> **Note**
>
> レビューテンプレートからワークロードを定義するには、ワークロードを作成するための IAM アクセス許可 `wellarchitected:CreateWorkload` および `wellarchitected:GetReviewTemplate`、`wellarchitected:GetReviewTemplateAnswer`、`w` のレビューテンプレート権限が有効になっている必要があります。IAM アクセス許可の詳細については、「AWS アイデンティティおよびアクセス管理ユーザーガイド」を参照してください。

レビューテンプレートからワークロードを定義するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. ワークロードを定義するレビューテンプレートの名前を選択します。
3. [テンプレートからワークロードを定義] を選択します。

   > **Note**
   >
   > [ワークロード] ページの [ワークロードの定義] ドロップダウンから [レビューテンプレートから定義] を選択することもできます。

4. [レビューテンプレートを選択] 手順で、レビューテンプレートカードを選択し、[次へ] を選択します。

5. [プロパティを指定] 手順で、ワークロードプロパティの必須フィールドを入力し、[次へ] を選択します。詳細については、「the section called “ワークロードの定義”」を参照してください。
6. (オプション) [プロファイルの適用] 手順では、既存のプロファイルを選択するか、プロファイル名を検索するか、[プロファイルを作成] を選択してプロファイルを作成し、プロファイルをワークロードに関連付けます。[次へ] をクリックします。

   Well-Architected プロファイルとレビューテンプレートは組み合わせて使用できます。レビューテンプレートに事前入力された質問はワークロードで引き続き回答され、質問にはプロファイルに基づいて優先順位が付けられます。
7. (オプション) [レンズを適用] 手順では、レビューテンプレートにまだ適用されていないレンズを、[カスタムレンズ] または [レンズカタログ] から追加で適用することもできます。
8. [ワークロードの定義] を選択します。

レビューテンプレートの削除

レビューテンプレートを削除するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. [レビューテンプレート] セクションで、削除するレビューテンプレートを選択し、[アクション] ドロップダウンで [削除] を選択します。

   > **Note**
   >
   > テンプレートの名前を選択し、レビューテンプレートの [概要] タブから [削除] を選択することもできます。
3. [レビューテンプレートを削除] ダイアログボックスにあるフィールドにレビューテンプレートの名前を入力し、削除を確認します。
4. [削除] をクリックします。

削除されたレビューテンプレートから新しいワークロードを作成することはできません。削除したレビューテンプレートを他の IAM ユーザー、アカウント、または組織と共有した場合、そのレビューテンプレートからワークロードを作成することはできません。

プロファイル

プロファイルを作成して、ビジネスコンテキストを提供すると、Well-Architected レビューを実施する際に達成したい目標を特定できます。AWS Well-Architected Tool は、プロファイルから収集した情報を使用して、ワークロードレビュー中にビジネスに関連する質問の優先リストに集中できるようにサポートします。ワークロードにプロファイルを添付すると、改善計画で対処すべき優先リスクを確認するのにも役立ちます。

[プロファイル] ページからプロファイルを作成して新しいワークロードに関連付けることも、既存のワークロードにプロファイルを追加することもできます。

プロファイルの作成

プロファイルを作成するには

1. 左側のナビゲーションペインで [プロファイル] を選択します。
2. [Create profile] (プロファイルの作成) を選択します。
3. [プロファイルのプロパティ] セクションで、プロファイルの [名前] と [説明] を入力します。
4. ワークロードレビューと改善計画の中でビジネスに対して優先度が高い情報を絞り込むには、[プロファイルに関する質問] セクションで、ビジネスに最も関連性がある回答を選択します。
5. (オプション) [タグ] セクションで、プロファイルに関連付けるタグを追加します。

   タグの詳細については、「AWS WA Tool リソースのタグ付け」を参照してください。
6. [保存] を選択します。プロファイルが正常に作成されると、成功メッセージが表示されます。

プロファイルが作成されると、プロファイルの概要が表示されます。概要には、名前、説明、ARN、作成日と更新日、プロファイルに関する質問への回答など、プロファイルに関連するデータが表示されます。[プロファイルの概要] ページでは、プロフィールを編集、削除、共有できます。

プロファイルの編集

プロファイルを編集するには

1. 左側のナビゲーションペインで [プロファイル] を選択するか、ワークロードの [プロファイル] セクションから [プロファイルを表示] を選択します。
2. 更新するプロファイルの名前を選択します。
3. [プロファイル概要] ページで [編集] を選択します。
4. プロファイルの質問に必要な更新を行います。
5. [保存] を選択します。

プロファイルの共有

プロファイルは、ユーザー、アカウント、組織全体、組織部門と共有できます。

プロファイルを共有するには

1. 左側のナビゲーションペインで [プロファイル] を選択します。
2. 共有するプロファイルの名前を選択します。
3. [共有] タブを選択します。
4. ユーザーまたはアカウントと共有するには、[作成] を選択し、[IAM ユーザーまたはアカウントへの共有を作成] を選択します。[招待を送信] ボックスで、ユーザー ID またはアカウント ID を指定し、[作成] を選択します。
5. 組織または組織部門と共有するには、[作成]、[Organizations への共有を作成] の順に選択します。組織全体で共有するには、[組織全体に許可を付与] を選択します。組織部門と共有するには、[個々の組織部門に許可を付与] を選択し、ボックスに組織部門を指定して、[作成] を選択します。

> **Important**
>
> プロファイルを組織または組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効にする必要があります。

ワークロードへのプロファイルの追加

既存のワークロードにプロファイルを追加するか、ワークロードを定義する際に、ワークロードレビュープロセスを加速できます。AWS WA Tool は、プロファイルから収集した情報を使用して、ビジネスに関連するワークロードレビューの質問に優先順位を付けます。

ワークロードを定義する際にプロファイルを追加する方法の詳細については、「the section called “ワークロードの定義”」を参照してください。

既存のワークロードにプロファイルを追加するには

1. 左側のナビゲーションペインで [ワークロード] を選択し、プロファイルに関連付けるワークロードの名前を選択します。

   > **Note**
   >
   > ワークロードに関連付けることができるプロファイルは 1 つだけです。

2. [プロファイル] セクションで [プロファイルの追加] を選択します。
3. 使用可能なプロファイルのリストからワークロードに適用するプロファイルを選択するか、[プロファイルの作成] を選択します。詳細については、「the section called “プロファイルの作成”」を参照してください。
4. [保存] を選択します。

[ワークロードの概要]には、関連するプロファイルの情報に基づいて、優先度の高い質問の回答数と優先度の高いリスクの数が表示されます。[レビューを続ける] を選択すると、ワークロードレビューで優先度の高い質問に回答できます。詳細については、「the section called “ワークロードのドキュメント化”」を参照してください。

[プロファイル] セクションには、ワークロードに関連付けられているプロファイルの名前、説明、ARN、バージョン、最終更新日が表示されます。

ワークロードからプロファイルを削除する

ワークロードからプロファイルを削除すると、そのワークロードはプロファイルが関連付けられていた以前のバージョンに戻り、ワークロードレビューの質問やリスクは優先されなくなります。

ワークロードからプロファイルを削除するには

1. ワークロードの [プロファイル] セクションで [削除] を選択します。
2. 削除を確認するには、テキスト入力フィールドにプロファイルの名前を入力します。
3. [Remove] (削除) を選択します。

プロファイルがワークロードから正常に削除されたことを示す通知が表示されます。ワークロードからプロファイルを削除すると、そのワークロードはプロファイルが関連付けられていた以前のバージョンに戻り、ワークロードレビューの質問やリスクは優先されなくなります。

AWS WA Tool からプロファイルを削除する

プロファイルを作成すると、AWS WA Tool で利用できるプロファイルのリストからそのプロファイルを削除できます。

[プロファイル] ページからプロファイルを削除しても、関連するワークロードからプロファイルは削除されません。削除前にワークロードと共有、関連付けられていたプロファイルは引き続き使用できますが、削除したプロファイルに新しいワークロードを関連付けることはできません。削除されたプロファイルを使用して the section called “プロファイル通知” がワークロード所有者に送信されます。

> **免責事項**
>
> 自分のプロファイルを他の AWS アカウント と共有することで、AWS が自分のプロファイルを他のアカウントで利用できることを認めたと見なされます。自分の AWS アカウント からプロファイルを削除したり、AWS アカウント を終了したとしても、これらの他のアカウントは、引き続き共有したプロファイルにアクセスして、使用できます。

プロファイルのリストからプロファイルを削除するには

1. 左側のナビゲーションペインで [プロファイル] を選択します。
2. 削除するプロファイルの名前を選択します。
3. [削除] を選択します。
4. 削除を確認するには、テキスト入力フィールドにプロファイルの名前を入力します。
5. [削除] を選択します。

プロファイルを [プロファイル] リストに残し、ワークロードからは削除したい場合は、「the section called “ワークロードからプロファイルを削除する”」を参照してください。

AWS Well-Architected Tool Connector for Jira

AWS Well-Architected Tool Connector for Jira を使用すると、Jira アカウントを にリンク AWS Well-Architected Tool し、ワークロードから改善項目を Jira プロジェクトに同期して、改善を実装するためのクローズドループメカニズムを作成できます。

コネクタは、自動同期と手動同期の両方を提供します。詳細については、「コネクタの設定」を参照してください。

コネクタは、アカウントレベルとワークロードレベルで設定でき、ワークロードごとにアカウントレベルの設定を上書きするオプションがあります。ワークロードレベルでは、ワークロードの同期を完全に除外することもできます。

改善項目をデフォルトの WA Jira プロジェクトに同期するか、同期する既存のプロジェクトキーを指定することができます。ワークロードレベルでは、必要に応じて各ワークロードを一意の Jira プロジェクトに同期できます。

> **Note**
>
> コネクタは Jira のスクラムプロジェクトとカンバンプロジェクトのみをサポートします。

改善項目が Jira に同期されると、次の方法で整理されます。

- プロジェクト： WA (または指定した既存のプロジェクト)
- エピック： ワークロード
- タスク： 質問
- サブタスク： ベストプラクティス
- ラベル： 柱

設定ページで Jira アカウントの同期を設定したら、Jira コネクタを設定し、改善項目を Jira アカウント に同期できます。

コネクタのセットアップ

コネクタをインストールするには

> **Note**
>
> 以下の手順はすべて、 ではなく Jira アカウントで実行されます AWS アカウント。

1. Jira アカウントにログインします。
2. 上部のナビゲーションバーで、アプリ を選択し、さらに多くのアプリを探索 を選択します。
3. Jira のアプリケーションと統合の検出ページで、 AWS 「 Well-Architected」と入力します。次に、 AWS Well-Architected Tool Connector for Jira を選択します。
4. アプリページで、アプリの取得 を選択します。
5. 「Jira に追加」ペインで、「今すぐ取得」を選択します。
6. アプリのインストール後、セットアップを完了するには、 の設定を選択します。
7. AWS Well-Architected Tool 設定ページで、新しい を接続するを選択します AWS アカウント。
8. AccessKeyId とシークレットキー を入力します。オプション: セッショントークン を入力します。次に、接続 を選択します。

> **Note**
>
> アカウントに アクセス許可 があることを確認します `wellarchitected:ConfigureIntegration`。このアクセス許可は Jira に追加 AWS アカウント するために必要です。
> 複数の を に接続 AWS アカウント できます AWS WA Tool。

> **Note**
>
> セキュリティのベストプラクティスとして、短期の IAM 認証情報を使用することを強くお勧めします。の AccessKeyIdとシークレットキーの作成の詳細については AWS アカウント、「アクセスキーの管理 (コンソール)」を参照してください。また、短期認証情報の使用の詳細については、「一時的な認証情報のリクエスト」を参照してください。

9. リージョン で、接続する AWS リージョン を選択します。次に、接続 を選択します。

Jira プロジェクトのセットアップ

カスタムプロジェクトを使用する場合は、プロジェクト設定に次の問題タイプがあることを確認してください。

- スクラム： エピック、ストーリー、サブタスク
- Kanban: エピック、タスク、サブタスク

問題タイプの管理の詳細については、「Atlassian Support | 問題タイプ の追加、編集、削除」を参照してください。

でコネクタのステータスを確認するには AWS Well-Architected Tool

1. にログイン AWS アカウント し、 に移動します AWS Well-Architected Tool。
2. 左側のナビゲーションペインで 設定 を選択します。
3. Jira アカウント同期セクションの Jira アプリ接続ステータス で、Configured ステータスを確認します。

これでコネクタがセットアップされ、設定する準備が整いました。アカウントおよびワークロードレベルで Jira 同期設定を構成するには、「コネクタ の設定」を参照してください。

コネクタの設定

AWS Well-Architected Tool Connector for Jira を使用すると、アカウントレベル、ワークロードレベル、またはその両方で Jira 同期を設定できます。アカウントレベルの設定に関係なくワークロードレベルの Jira 設定を構成することも、特定のワークロードのアカウントレベルの設定を上書きしてワークロードの同期動作を指定することもできます。ワークロード を定義するときに Jira 設定を構成することもできます。

コネクタには、自動同期と手動同期の 2 つの同期方法があります。どちらの同期方法でも、 で行われた変更は Jira プロジェクト AWS WA Tool に反映され、Jira で行われた変更は に同期されます AWS WA Tool。

> **Important**
>
> 自動同期を使用すると、Jira の変更に応じてワークロード AWS WA Tool を変更することに同意したものと見なされます。
> Jira に同期したくない機密情報がある場合は、ワークロードのメモフィールドにこの情報を入力しないでください。

- 自動同期： コネクタは、ベストプラクティスの選択または選択解除や質問の完了など、質問が更新されるたびに Jira プロジェクトとワークロードを自動的に更新します。
- 手動同期： Jira と の間で改善項目を同期する場合は、ワークロードダッシュボードで Jira と同期を選択する必要があります AWS WA Tool。同期する特定の柱と質問を選択することもできます。詳細については、「ワークロードの同期」を参照してください。

アカウントレベルでコネクタを設定するには

1. 左側のナビゲーションペインで 設定 を選択します。
2. Jira アカウント同期ペインで、編集 を選択します。
3. 同期タイプ で、次のいずれかを選択します。
   a. 変更が行われたときにワークロードを自動的に同期するには、自動 を選択します。
   b. ワークロードを同期するタイミングを手動で選択するには、手動 を選択します。
4. デフォルトでは、コネクタは WA Jira プロジェクトを作成します。独自の Jira プロジェクトキーを指定するには、次の手順を実行します。
   a. 「デフォルトの Jira プロジェクトキーを上書きする」を選択します。
   b. Jira プロジェクトキー を入力します。

   > **Note**
   >
   > 指定された Jira プロジェクトキーは、ワークロードレベルでプロジェクトを変更しない限り、すべてのワークロードに使用されます。

5. [設定を保存] を選択します。

ワークロードレベルでコネクタを設定するには

1. 左側のナビゲーションペインでワークロードを選択し、設定するワークロードの名前を選択します。
2. [プロパティ] を選択します。
3. Jira ペインで、編集 を選択します。
4. ワークロードの Jira 設定を構成するには、アカウントレベルの設定を上書きする を選択します。

   > **Note**
   >
   > ワークロード固有の設定を適用するには、アカウントレベルの設定を上書きする必要があります。

5. 同期オーバーライド で、次のいずれかを選択します。

   a. Jira 同期からワークロードを除外するには、ワークロードを同期しない を選択します。

   b. ワークロードを同期するタイミングを手動で選択するには、ワークロードの同期 - 手動 を選択します。

   c. ワークロードの変更を自動的に同期するには、ワークロードの同期 - 自動 を選択します。

6. (オプション) Jira プロジェクトキー には、ワークロードを同期するプロジェクトキーを入力します。このプロジェクトキーは、アカウントレベルのプロジェクトキーとは異なる場合があります。

   プロジェクトキーを指定しない場合、コネクタは WA Jira プロジェクトを作成します。

7. [保存] を選択します。

手動同期の実行の詳細については、「ワークロードの同期」を参照してください。

ワークロードの同期

自動同期の場合、コネクタはワークロードを更新するときに改善項目を自動的に同期します (例えば、質問を完了したり、新しいベストプラクティスを選択したりするなど) 。

手動同期と自動同期の両方で、Jira で行われた変更 (質問の完了やベストプラクティスなど) は に同期されます AWS Well-Architected Tool。

ワークロードを手動で同期するには

1. ワークロードを Jira に同期する準備ができたら、左側のナビゲーションペインでワークロードを選択します。次に、同期するワークロードを選択します。
2. ワークロードの概要で、Sync with Jira を選択します。
3. 同期するレンズを選択します。
4. Jira に同期する質問 については、Jira プロジェクトに同期する質問または柱全体を選択します。
   - 削除する質問については、質問タイトルの横にある X アイコンを選択します。
5. 同期 を選択します。

コネクタのアンインストール

AWS Well-Architected Tool Connector for Jira を完全にアンインストールするには、次のタスクを実行します。

- アカウントレベルの同期設定を上書きするワークロードで Jira 同期を無効にする
- アカウントレベルで Jira 同期をオフにする
- Jira AWS アカウント で のリンクを解除する
- Jira アカウントからコネクタをアンインストールする

アカウントレベルでコネクタをオフにするには

> **Note**
>
> 以下の手順は、 で実行されます AWS アカウント。

1. 左側のナビゲーションペインで 設定 を選択します。
2. Jira アカウント同期セクションで、編集 を選択します。
3. Jira アカウント同期を有効にするオプションをクリアします。
4. [設定を保存] を選択します。

のリンクを解除するには AWS アカウント

> **Note**
>
> 以下の手順はすべて、 ではなく Jira アカウントで実行されます AWS アカウント。

1. Jira アカウントにログインします。
2. 上部のナビゲーションバーで、アプリ を選択し、アプリの管理 を選択します。
3. AWS Well-Architected Tool Connector for Jira の横にあるドロップダウン矢印を選択し、Configure を選択します。
4. AWS Well-Architected Tool 設定ペインで、 のリンクを解除するには AWS アカウント、アクション で X を選択します。

コネクタをアンインストールするには

> **Note**
>
> 以下の手順はすべて、 ではなく Jira アカウントで実行されます AWS アカウント。
> コネクタをアンインストールする前に AWS アカウント 、接続されているすべてのリンクがコネクタの設定で解除されていることを確認することをお勧めします。

1. Jira アカウントにログインします。
2. 上部のナビゲーションバーで、アプリ を選択し、アプリの管理 を選択します。
3. AWS Well-Architected Tool Connector for Jira の横にあるドロップダウン矢印を選択します。
4. アンインストール を選択し、アプリのアンインストール を選択します。

マイルストーン

マイルストーンは、特定の時点におけるワークロードの状態を記録します。

最初に、ワークロードに関連するすべての質問を完了したら、マイルストーンを保存します。改善計画の項目に基づいてワークロードを変更するときに、進捗状況を評価するための追加のマイルストーンを保存できます。

ベストプラクティスは、ワークロードを改善するたびにマイルストーンを保存することです。

マイルストーンの保存

マイルストーンには、ワークロードの現在のステータスが記録されます。ワークロードの所有者は、いつでもマイルストーンを保存できます。

マイルストーンを保存するには

1. ワークロード詳細ページで、[Save milestone (マイルストーンの保存)] を選択します。
2. [Milestone name (マイルストーン名)] ボックスに、マイルストーンの名前を入力します。

   > **Note**
   >
   > 名前は 3 ~ 100 文字にしてください。3 文字以上をスペースにしないでください。ワークロードに関連付けられるマイルストーン名は一意にしてください。一意かどうかを確認するときは、スペースと大文字の使用は無視されます。

3. [Save (保存)] を選択してマイルストーンを保存します。

マイルストーンが保存された後は、記録されたワークロードデータを変更することはできません。ワークロードを削除すると、それに関連付けられているマイルストーンも削除されます。

マイルストーンの表示

以下の方法で、ワークロードのマイルストーンを表示できます。

- ワークロード詳細ページで、[Milestones (マイルストーン)] を選択してから、表示するマイルストーンを選択します。

- [Dashboard (ダッシュボード)] ページの [Milestones (マイルストーン)] セクションでワークロードを選択してから、表示するマイルストーンを選択します。

マイルストーンレポートの生成

マイルストーンレポートを生成できます。このレポートには、ワークロードの質問、メモ、およびマイルストーンが保存された時点で存在していた中および高リスクに対する応答が含まれます。

レポートを使用すると、AWS Well-Architected Tool にアクセスできない他のユーザーとマイルストーンに関する詳細を共有できます。

マイルストーンレポートを生成するには

1. 以下のいずれかの方法でマイルストーンを選択します。
   - ワークロード詳細ページで、[Milestones (マイルストーン)] を選択してから、マイルストーンを選択します。
   - [Dashboard (ダッシュボード)] ページで、レポートするマイルストーンのワークロードを選択します。[Milestones (マイルストーン)] セクションで、マイルストーンを選択します。
2. [レポートの生成] を選択してレポートを生成します。

   PDF ファイルが生成され、そのダウンロードや表示が可能になります。

共有の招待

共有の招待は、別の AWS アカウントが所有するワークロード、カスタムレンズまたはレビューテンプレートを共有するためのリクエストです。ワークロードまたはレンズは、AWS アカウント のすべてのユーザー、個々のユーザー、またはその両方と共有できます。

- ワークロードの招待を承諾すると、そのワークロードが [Workloads] (ワークロード) ページと [Dashboard] (ダッシュボード) ページに追加されます。
- カスタムレンズの招待を承諾すると、そのレンズが [Custom lenses] (カスタムレンズ) ページに追加されます。
- プロフィールの招待を承諾すると、[プロファイル] ページにプロファイルが追加されます。
- レビューテンプレートの招待を承諾すると、[レビューテンプレート] ページにテンプレートが追加されます。

招待を拒否すると、一覧から削除されます。

> **Note**
>
> ワークロード、カスタムレンズ、プロファイルおよびレビューテンプレートは、同じ AWS リージョン 内でのみ共有できます。

ワークロードまたはカスタムレンズの所有者は、共有アクセス権を持つユーザーを管理します。

左側のナビゲーションからアクセスできる [Share invitations] (共有の招待) ページには、ワークロードとカスタムレンズの保留中の招待に関する情報が表示されます。

ワークロードの招待ごとに以下の情報が表示されます。

名前

共有するワークロード、カスタムレンズ、またはレビューテンプレートの名前。

リソースタイプ

招待のタイプ (ワークロード、カスタムレンズ、プロファイル、レビューテンプレートのいずれか)。

所有者

ワークロードを所有する AWS アカウント ID。

アクセス許可

ワークロードに対してユーザーに付与されているアクセス許可。

- 読み取り専用

  ワークロード、カスタムレンズ、プロファイルまたはレビューテンプレートへの読み取り専用アクセスを提供します。

- 投稿者

  回答とそのメモへの更新アクセスと、残りのワークロードへの読み取り専用アクセスを許可します。このアクセス許可は、ワークロードの場合にのみ使用できます。

アクセス許可の詳細

アクセス許可の詳細説明。

共有の招待の承諾

共有の招待を承諾するには

1. 承諾する共有の招待を選択します。
2. [Accept] (承諾) を選択します。

ワークロードの招待の場合は、そのワークロードが [Workloads] (ワークロード) ページと [Dashboard] (ダッシュボード) ページに追加されます。カスタムレンズの招待の場合は、そのカスタムレンズが [Custom lenses] (カスタムレンズ) ページに追加されます。プロファイル招待の場合、[プロファイル] ページにプロファイルが追加されます。レビューテンプレートの招待の場合、[レビューテンプレート] ページにテンプレートが追加されます。

招待を承諾するまで 7 日間の猶予があります。7 日以内に招待を承諾しない場合は、自動的に期限切れになります。

ユーザーと AWS アカウント の両方がワークロード招待を承諾した場合、ユーザーのワークロード招待がユーザーのアクセス許可を判断します。

共有の招待の拒否

共有の招待を拒否するには

1. 拒否するワークロードまたはカスタムレンズの招待を選択します。
2. [拒否] を選択します。

招待がリストから削除されます。

通知

[通知] ページには、ワークロードのバージョンの違いと、レンズとプロファイルが関連付けられているレビューテンプレートが表示されます。[通知] ページでは、ワークロードのレンズまたはプロファイルの最新バージョンにアップグレードできます。

レンズ通知

新しいバージョンのレンズが利用可能になると、[ワークロード] ページまたは [レビューテンプレート] ページの上部にバナーが表示され、通知されます。古いレンズを使用する特定のワークロードまたはレビューテンプレートを表示している場合も、新しいバージョンのレンズが利用可能であることを示すバナーが表示されます。

アップグレード可能なワークロードまたはレビューテンプレートのリストに対して、[利用可能なアップグレードを表示] を選択します。

ワークロードまたはレビューテンプレートにレンズをアップグレードする手順については、「the section called “レンズのアップグレード”」を参照してください。

共有レンズの所有者がレンズを削除したときに、削除したレンズに関連するワークロードがある場合は、既存のワークロードではレンズを引き続き使用できますが、新しいワークロードには追加できないという通知が届きます。

プロファイル通知

プロファイル通知には、次の 2 種類があります。

- プロファイルのアップグレード
- プロファイルの削除

ワークロードに関連付けられているプロファイルが編集されると (詳細については、「the section called “プロファイルの編集”」を参照)、プロファイルの新しいバージョンがあるという通知が [プロファイル通知] に表示されます。

共有プロファイルの所有者がプロファイルを削除したときに、削除したプロファイルに関連するワークロードがある場合は、既存のワークロードではプロファイルを引き続き使用できますが、新しいワークロードには追加できないという通知が届きます。

プロファイルバージョンをアップグレードするには

1. 左側のナビゲーションペインで、[通知] を選択します。
2. [プロファイル通知] タブのリストからワークロードの名前を選択するか、検索バーを使用してワークロード名で検索します。
3. [プロファイルバージョンのアップグレード] を選択します。
4. [承認] セクションで、[これらの変更を理解し、受け入れます] の確認ボックスを選択します。
5. (オプション) マイルストーンを保存する場合は、[マイルストーンを保存] ボックスを選択し、[マイルストーン名] を指定します。
6. [保存] を選択します。

プロファイルがアップグレードされると、最新のバージョン番号と更新日がワークロードの [プロファイル] セクションに表示されます。

詳細については、「プロファイル」を参照してください。

ダッシュボード

左側のナビゲーションで使用可能な [ダッシュボード] では、ワークロードとそれらに関連付けられている中リスクの問題および高リスクの問題にアクセスできます。自分と共有されているワークロードを含めることもできます。[ダッシュボード] は 4 つのセクションで構成されます。

- 概要 — すべてのワークロードにおけるワークロードの総数、高リスクと中リスクが割り当てられている数、および高リスクと中リスクの問題の合計数が表示されます。
- Well-Architected フレームワークの柱ごとの問題 — すべてのワークロードについて、高リスクと中リスクの問題を柱ごとにグラフィカルに表示します。
- Well-Architected フレームワークのワークロードごとの問題 — 各ワークロードの高リスクと中リスクの問題を柱ごとに表示します。
- Well-Architected フレームワークの改善計画項目ごとの問題 — すべてのワークロードの改善計画項目を表示します。

まとめ

このセクションには、Well-Architected フレームワークレンズと他のすべてのレンズ内の、ワークロードの総数と、高リスクと中リスクの問題があるワークロードの数が表示されます。所有または AWS アカウント と共有しているすべてのワークロードにおける高リスクと中リスクの問題の合計数が表示されます。

[自分と共有されているワークロードを含める] を選択すると、統計の概要、統合レポート、およびその他のダッシュボードセクションに、自分のワークロードと自分と共有されているワークロードの両方が反映されます。

[レポートの生成] を選択すると、統合レポートが PDF ファイルとして作成されます。

レポート名の形式は、`wellarchitected_consolidatedreport_`*`account-ID`*`.pdf` です。

Well-Architected フレームワークの柱ごとの問題

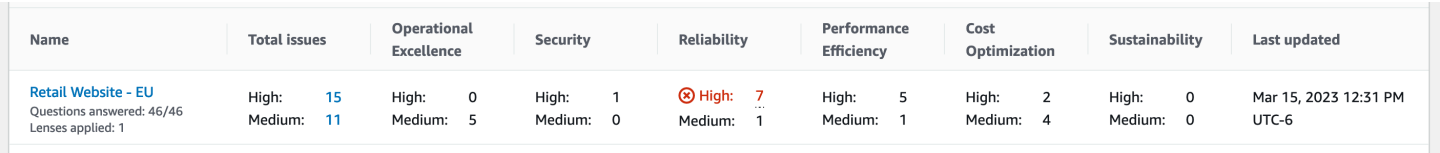
[Well-Architected フレームワークの柱ごとの問題] セクションでは、すべてのワークロードにおける高リスクおよび中リスクの問題の数を柱ごとにグラフで表示しています。

ダッシュボードの残りのセクションを使用すると、ある詳細レベルから次の詳細レベルに移動できます。

> **Note**
>
> このセクションには、Well-Architected フレームワークレンズからの問題のみが含まれています。

Well-Architected フレームワークのワークロードごとの問題

[Well-Architected フレームワークのワークロードごとの問題] セクションには、各ワークロードの情報が表示されます。



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

ワークロードごとに以下の情報が表示されます。

名前

ワークロードの名前。回答された質問の数と、ワークロードに適用されたレンズの数も表示されます。

ワークロード名を選択すると、[ワークロードの詳細] ページにアクセスして、マイルストーン、改善計画、共有を確認できます。

総問題数

ワークロード用 Well-Architected フレームワークレンズが特定した問題の総数。

高リスクまたは中リスクの問題の数を選択すると、それらの問題に対する推奨改善計画が表示されます。

オペレーショナルエクセレンス

運用上の優秀性の柱用ワークロードで特定された高リスクの問題 (HRI) および中リスクの問題 (MRI) の数。

セキュリティ

セキュリティの柱で特定された HRI と MRI の数。

信頼性

信頼性の柱で特定された HRI と MRI の数。

パフォーマンス効率

パフォーマンス効率の柱で特定された HRI と MRI の数。

コスト最適化

コスト最適化の柱で特定された HRI と MRI の数。

サステナビリティ

サステナビリティの柱で特定された HRI と MRI の数。

最終更新日

ワークロードが最後に更新された日時。

各ワークロードについて、高リスクの問題 (HRI) の数が最も多い柱が強調表示されます。

> **Note**
>
> このセクションには、Well-Architected フレームワークレンズからの問題のみが含まれています。

Well-Architected フレームワークの改善計画項目ごとの問題

[Well-Architected フレームワークの改善計画項目ごとの問題] セクションには、すべてのワークロードの改善計画項目が表示されます。項目は柱と重要度に基づいてフィルタリングできます。

各改善計画項目に対して以下の情報が表示されます。

改善項目

改善計画項目の名前。

改善計画項目に関連するベストプラクティスを示す名前を選択します。

柱

改善項目に関連する柱。

Risk

関連する問題が高リスクか中リスクかを示します。

該当するワークロード

この改善計画が適用されるワークロードの数。

改善計画項目を選択すると、該当するワークロードが表示されます。

> **Note**
>
> このセクションには、Well-Architected フレームワークレンズの改善計画項目のみが含まれます。

のセキュリティ AWS Well-Architected Tool

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルではこれを、クラウドのセキュリティ、およびクラウド内でのセキュリティと説明しています:

- クラウドのセキュリティ — AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。また、 は、安全に使用できるサービス AWS も提供します。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。に適用されるコンプライアンスプログラムの詳細については AWS Well-Architected Tool、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS WA Tool。以下のトピックでは、セキュリティおよびコンプライアンスの目的 AWS WA Tool を達成するために を設定する方法を示します。また、 AWS WA Tool リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

でのデータ保護 AWS Well-Architected Tool

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Well-Architected Tool。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された記事「AWS 責任共有モデルおよび GDPR」を参照してください。

データ保護の目的で、 認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、AWS WA Tool または SDK を使用して AWS CLIまたは他の AWS のサービス を操作する場合も同様です。 AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

保管中の暗号化

によって保存されるすべてのデータは AWS WA Tool 、保管時に暗号化されます。

転送中の暗号化

との間で送受信されるすべてのデータは AWS WA Tool 、転送中に暗号化されます。

AWS がデータを使用する方法

AWS Well-Architected チームは から集約データを収集 AWS Well-Architected Tool し、お客様に AWS WA Tool サービスを提供し、改善します。個々の顧客データはチームと共有 AWS アカウントされ、ワークロードとアーキテクチャを改善するためのお客様の取り組みをサポートする場合があります。 AWS Well-Architected チームは、各質問のワークロードプロパティと選択した選択肢にのみアクセスできます。 の AWS WA Tool 外部からのデータは共有 AWS されません AWS。

AWS Well-Architected チームがアクセスできるワークロードプロパティには、以下が含まれます。

- ワークロード名
- レビュー所有者
- 環境
- リージョン
- アカウント ID
- 業種タイプ

AWS Well-Architected チームは以下にアクセスできません。

- ワークロードの説明
- アーキテクチャの設計
- 入力されたメモ

の Identity and Access Management AWS Well-Architected Tool

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS WA Tool リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- 対象者

- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- が IAM と AWS Well-Architected Tool 連携する方法
- AWS Well-Architected Tool アイデンティティベースのポリシーの例
- AWS の マネージドポリシー AWS Well-Architected Tool
- AWS Well-Architected Tool ID とアクセスのトラブルシューティング

対象者

AWS Identity and Access Management (IAM) の使用方法は、 で行う作業によって異なります AWS WA Tool。

サービスユーザー – AWS WA Tool サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AWS WA Tool 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者から適切な権限をリクエストするのに役に立ちます。 AWS WA Tool機能にアクセスできない場合は、「AWS Well-Architected Tool ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内の AWS WA Tool リソースを担当している場合は、通常、 へのフルアクセスがあります AWS WA Tool。サービスユーザーがどの AWS WA Tool 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で IAM を で使用する方法の詳細については、 AWS WA Tool「」を参照してくださいが IAM と AWS Well-Architected Tool 連携する方法。

IAM 管理者 - 管理者は、 AWS WA Toolへのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。IAM で使用できる AWS WA Tool アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Well-Architected Tool アイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（ IAM Identity Center) ユーザー、会社のシングルサインオン

認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 にサインインする方法 AWS アカウントAWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、『AWS IAM Identity Center ユーザーガイド』の「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、『IAM ユーザーガイド』の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、Identity Center ディレクトリのユーザー、または ID ソースを通じて提供さ

れた認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がにアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、『AWS IAM Identity Center ユーザーガイド』の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する権限を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、『IAM ユーザーガイド』の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細に

ついては、「IAM ユーザーガイド」の「AWS のサービスに権限を委任するロールの作成」を参照してください。

- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、『IAM ユーザーガイド』の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) AWS がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、『IAM ユーザーガイド』の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーで IAM の AWS マネージドポリシーを使用することはできません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、『Amazon Simple Storage Service デベロッパーガイド』の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

が IAM と AWS Well-Architected Tool 連携する方法

IAM を使用して へのアクセスを管理する前に AWS WA Tool、 で使用できる IAM 機能について学びます AWS WA Tool。

で使用できる IAM の機能 AWS Well-Architected Tool

IAM 機能	AWS WA Tool サポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	No
ポリシーアクション	Yes
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	No
ABAC (ポリシー内のタグ)	はい
一時的な認証情報	Yes
プリンシパル権限	Yes
サービスロール	いいえ
サービスリンクロール	いいえ

AWS WA Tool およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」の「IAM AWS と連携する のサービス」を参照してください。

AWS WA Tool アイデンティティベースのポリシー

ポリシーアクションのサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーのAction要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

内のリソースベースのポリシー AWS WA Tool

リソースベースのポリシーのサポート	No

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

のポリシーアクション AWS WA Tool

ポリシーアクションに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーのAction要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

のポリシーアクションは、アクションの前にプレフィックス AWS WA Tool を使用しますwellarchitected:。たとえば、エンティティがワークロードを定義できるようにするには、管理者は wellarchitected:CreateWorkload アクションを許可するポリシーをアタッチする必要があります。同様に、エンティティによるワークロードの削除を防止するため、管理者は wellarchitected:DeleteWorkload アクションを拒否するポリシーをアタッチできます。ポリシーステートメントには、Action 要素または NotAction 要素のいずれかを含める必要があります。 AWS WA Tool は、このサービスで実行できるタスクを説明する独自の一連のアクションを定義します。

AWS WA Tool アクションのリストを確認するには、「サービス認証リファレンス」の「 で定義されるアクション AWS Well-Architected Tool」を参照してください。

ポリシーリソース

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

AWS WA Tool リソースタイプとその ARNs」の「 で定義されるリソース AWS Well-Architected Tool」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、「AWS Well-Architected Toolで定義されるアクション」を参照してください。

AWS WA Tool ワークロードリソースには次の ARN があります。

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

ARN の形式の詳細については、「Amazon リソースネーム (ARNs AWS 「サービス名前空間」を参照してください。

ARN は、ワークロードの [ワークロードのプロパティ] ページにあります。たとえば、特定のワークロードを指定するには、次のようにします。

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

特定のアカウントに属するすべてのワークロードを指定するには、ワイルドカード (*) を使用します。

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

ワークロードの作成や一覧表示などの一部の AWS WA Tool アクションは、特定のリソースで実行できません。このような場合は、ワイルドカード *を使用する必要があります。

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

AWS WA Tool リソースタイプとその ARNs」の「 で定義されるリソース AWS Well-Architected Tool」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、「AWS Well-Architected Toolで定義されるアクション」を参照してください。

のポリシー条件キー AWS WA Tool

サービス固有のポリシー条件キーのサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

AWS WA Tool は 1 つのサービス固有の条件キー (wellarchitected:JiraProjectKey) を提供し、一部のグローバル条件キーの使用をサポートします。すべての AWS グローバル条件キーを確認するには、「サービス認証リファレンス」のAWS 「グローバル条件コンテキストキー」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細

については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

ACLs AWS WA Tool

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

AWS WA Tool タグに基づく認可

ABAC のサポート (ポリシー内のタグ)	はい

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義するアクセス許可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合に操作を許可するように ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、『IAM ユーザーガイド』の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性に基づくアクセスコントロール (ABAC) を使用する」を参照してください。

での一時的な認証情報の使用 AWS WA Tool

一時的な認証情報のサポート	はい

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

のクロスサービスプリンシパル許可 AWS WA Tool

フォワードアクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FASリクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS WA Toolのサービスロール

サービスロールのサポート	いいえ

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに権限を委任するロールの作成」を参照してください。

のサービスにリンクされたロール AWS WA Tool

サービスにリンクされたロールのサポート	いいえ

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[Yes] リンクを選択します。

AWS Well-Architected Tool アイデンティティベースのポリシーの例

デフォルトでは、 ユーザーおよびロールには、 AWS WA Tool リソースを作成または変更する権限はありません。また、、 AWS Management Console AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらのアクセス許可が必要なユーザーまたはグループにそのポリシーをアタッチします。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

トピック

- ポリシーのベストプラクティス
- AWS WA Tool コンソールを使用する
- ユーザーが自分の許可を表示できるようにする
- ワークロードへのフルアクセスの付与
- ワークロードへの読み取り専用アクセスの付与
- 1 つのワークロードへのアクセス
- サービス固有の条件キーの使用

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AWS WA Tool リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、『IAM ユーザーガイド』の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権権限とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、『IAM ユーザーガイド』の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサ

ポートします。詳細については、『IAM ユーザーガイド』の「IAM Access Analyzer ポリシーの検証」を参照してください。

- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、『IAM ユーザーガイド』の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

AWS WA Tool コンソールを使用する

AWS Well-Architected Tool コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の AWS WA Tool リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

これらのエンティティが AWS WA Tool 引き続きコンソールを使用できるようにするには、エンティティに次の AWS 管理ポリシーもアタッチします。

```
WellArchitectedConsoleReadOnlyAccess
```

ワークロードを作成、変更、および削除するためには、次の AWS 管理ポリシーをエンティティにアタッチします。

```
WellArchitectedConsoleFullAccess
```

詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、

または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

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

ワークロードへのフルアクセスの付与

この例では、 のユーザーにワークロードへの AWS アカウント フルアクセスを付与します。フルアクセスにより、ユーザーは ですべてのアクションを実行できます AWS WA Tool。このアクセスは、ワークロードの定義、ワークロードの削除、ワークロードの表示、ワークロードの更新に必要です。

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

ワークロードへの読み取り専用アクセスの付与

この例では、ワークロードへの AWS アカウント 読み取り専用アクセスをユーザーに許可します。読み取り専用アクセスでは、ユーザーは AWS WA Toolのワークロードを表示できるのみです。

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

1 つのワークロードへのアクセス

この例では、 us-west-2リージョンのワークロードの 1 つである への AWS アカウント 読み取り専用アクセスを99999999999955555555555566666666ユーザーに付与します。お客様のアカウント ID は 777788889999 です。

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

```
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555666666666"
     }
   ]
}
```

サービス固有の条件キーの使用

この例では、サービス固有の条件キーを使用して`wellarchitected:JiraProjectKey`、 AWS Well-Architected Tool Connector for Jira の統合と設定の詳細を取得できます。

```
{
 "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": "SOME_WORKLOAD_ARN",
   "Condition": {
    "StringEqualsIfExists": {
```

```
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
   }
  }
 ]
}
```

AWS の マネージドポリシー AWS Well-Architected Tool

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 AWS は、新しい AWS のサービス が起動されたとき、または既存のサービスで新しい API オペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS 管理ポリシー: WellArchitectedConsoleFullAccess

`WellArchitectedConsoleFullAccess` ポリシーは IAM ID にアタッチできます。

このポリシーは、 へのフルアクセスを許可します AWS Well-Architected Tool。

許可の詳細

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

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

AWS マネージドポリシー: WellArchitectedConsoleReadOnlyAccess

`WellArchitectedConsoleReadOnlyAccess` ポリシーは IAM ID にアタッチできます。

このポリシーは、 への読み取り専用アクセスを許可します AWS Well-Architected Tool。

許可の詳細

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

AWS マネージドポリシー: AWSWellArchitectedOrganizationsServiceRolePolicy

`AWSWellArchitectedOrganizationsServiceRolePolicy` ポリシーは IAM ID にアタッチできます。

このポリシーは AWS Organizations 、Organizations と AWS Well-Architected Tool の統合をサポートするために必要な の管理アクセス許可を付与します。これらのアクセス許可により、組織管理アカウントは とのリソース共有を有効にできます AWS WA Tool。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- organizations:ListAWSServiceAccessForOrganization — プリンシパルが AWS のサービスアクセスが有効になっているかどうかを確認できます AWS WA Tool。
- organizations:DescribeAccount - 組織内のアカウントに関する情報の取得をプリンシパルに許可します。
- organizations:DescribeOrganization - 組織設定に関する情報の取得を、プリンシパルに許可します。
- organizations:ListAccounts - 組織に属するアカウントリストの取得を、プリンシパルに許可します。
- organizations:ListAccountsForParent - 組織に属するアカウントのリストを組織の指定ルートノードから取得することをプリンシパルに許可します。
- organizations:ListChildren - 組織に属するアカウントのリストの組織部門を組織の指定ルートノードから取得することをプリンシパルに許可します。
- organizations:ListParents - 組織内の OU またはアカウントで指定された直属の親リストの取得をプリンシパルに許可します。
- organizations:ListRoots - 組織内のすべてのルートノードの一覧の取得をプリンシパルに許可します。

```
{
    "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 管理ポリシー： AWSWellArchitectedDiscoveryServiceRolePolicy

AWSWellArchitectedDiscoveryServiceRolePolicy ポリシーは IAM ID にアタッチできます。

このポリシーにより、 AWS Well-Architected Tool は リソースに関連する AWS サービスと AWS WA Tool リソースにアクセスできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- trustedadvisor:DescribeChecks – 利用可能な Trusted Advisor チェックを一覧表示します。
- trustedadvisor:DescribeCheckItems – によってフラグが付けられたステータスやリソースなどの Trusted Advisor チェックデータを取得します Trusted Advisor。
- servicecatalog:GetApplication – AppRegistry アプリケーションの詳細を取得します。
- servicecatalog:ListAssociatedResources – AppRegistry アプリケーションに関連付けられたリソースを一覧表示します。
- cloudformation:DescribeStacks — AWS CloudFormation スタックの詳細を取得します。
- cloudformation:ListStackResources – AWS CloudFormation スタックに関連付けられたリソースを一覧表示します。
- resource-groups:ListGroupResources - からのリソースを一覧表示します ResourceGroup。
- tag:GetResources – に必要です ListGroupResources。
- servicecatalog:CreateAttributeGroup — 必要に応じてサービス管理属性グループを作成します。
- servicecatalog:AssociateAttributeGroup – サービスマネージド属性グループを AppRegistry アプリケーションに関連付けます。
- servicecatalog:UpdateAttributeGroup — サービス管理属性グループを更新します。
- servicecatalog:DisassociateAttributeGroup - サービスマネージド属性グループと AppRegistry アプリケーションとの関連付けを解除します。
- servicecatalog:DeleteAttributeGroup — 必要に応じてサービス管理属性グループを削除します。

```
{
 "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 ToolAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AWS WA Tool 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートを受け取るには、 AWS WA Tool ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWS WA Tool 管理ポリシーの変更	`"wellarchitected:Export*"` が `WellArchitectedConsoleReadOnlyAccess` に追加されました。	2023 年 6 月 22 日
AWS WA Tool がサービスロールポリシーを追加	`AWSWellArchitectedDiscoveryServiceRolePolicy` AWS Well-Architected Tool が リソースに関連する AWS サービスと AWS WA Tool リソースにアクセスできるように を追加しました。	2023 年 5 月 3 日

変更	説明	日付
AWS WA Tool がアクセス許可を追加しました	AWS がサービスアクセスが AWS WA Tool に対して有効になっているかどうかを確認するListAWSServiceAccessForOrganization ために、 に付与する新しいアクションを追加しました AWS WA Tool。	2022 年 7 月 22 日
AWS WA Tool が変更の追跡を開始しました	AWS WA Tool が AWS マネージドポリシーの変更の追跡を開始しました。	2022 年 7 月 22 日

AWS Well-Architected Tool ID とアクセスのトラブルシューティング

次の情報は、 と IAM の使用時に発生する可能性がある一般的な問題の診断 AWS WA Tool と修正に役立ちます。

トピック

- でアクションを実行する権限がない AWS WA Tool

でアクションを実行する権限がない AWS WA Tool

がアクションを実行する権限がないと AWS Management Console 通知した場合は、管理者に連絡してサポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当者です。

以下の例のエラーは、*mateojackson* ユーザーがコンソールを使用して、DeleteWorkload アクションを実行しようとしたが、アクセス許可がない場合に発生します。

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

この例の場合は、wellarchitected:DeleteWorkload アクションを使用して 11112222333344445555666677778888 リソースへのアクセスを許可するように、管理者にポリシーを更新してもらいます。

でのインシデント対応 AWS Well-Architected Tool

のインシデント対応 AWS Well-Architected Tool は AWS 責任です。 AWS には、インシデント対応を管理する正式な文書化されたポリシーとプログラムがあります。

AWS 広範な影響を与える運用上の問題は、AWS Service Health Dashboard に投稿されます。

運用上の問題も、 AWS Health Dashboardを介して個々のアカウントに投稿されます。の使用方法については AWS Health Dashboard、「 AWS Health ユーザーガイド」を参照してください。

のコンプライアンス検証 AWS Well-Architected Tool

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

  > **Note**
  >
  > すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。

- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 AWS Well-Architected Tool

AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供し、低レイテンシー、高スループット、高冗長ネットワークで接続されます。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS Well-Architected Tool

マネージドサービスである AWS Well-Architected Tool は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開している API コールを使用して、ネットワーク AWS WA Tool 経由で にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

での設定と脆弱性の分析 AWS Well-Architected Tool

設定と IT コントロールは、 AWS とお客様の間の責任共有です。詳細については、 AWS 「 責任共有モデル」を参照してください。

サービス間での不分別な代理処理の防止

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐために、 AWS には、アカウント内のリソースへのアクセス権が付与されたサービスプリンシパルですべてのサービスのデータを保護するために役立つツールが用意されています。

リソースポリシーで aws:SourceArnおよび aws:SourceAccount グローバル条件コンテキストキーを使用して、 が別のサービスに AWS Well-Architected Tool 付与するアクセス許可をリソースに制限することをお勧めします。クロスサービスアクセスにリソースを 1 つだけ関連付けたい場合は、aws:SourceArn を使用します。そのアカウント内のリソースをクロスサービスの使用に関連付けることを許可する場合は、aws:SourceAccount を使用します。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して、aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合には、グローバルコンテキスト条件キー aws:SourceArn で、ARN の未知部分を示すためにワイルドカード文字 (*) を使用します。例えば、arn:aws:wellarchitected:*:*123456789012*:* です。

aws:SourceArn の値に Amazon S3 バケット ARN などのアカウント ID が含まれていない場合は、両方のグローバル条件コンテキストキーを使用して、アクセス許可を制限する必要があります。

aws:SourceArn の値はワークロードかレンズにする必要があります。

次の例は、 で aws:SourceArnおよび aws:SourceAccount グローバル条件コンテキストキーを使用して、混乱した代理問題 AWS WA Tool を回避する方法を示しています。

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

AWS WA Tool リソースの共有

所有しているリソースを共有するには、次の手順を実行します。

- AWS Organizations 内でリソース共有を有効にする (オプション)
- ワークロードを共有する
- カスタムレンズを共有する
- プロフィールを共有する
- レビューテンプレートを共有する

> **メモ**
>
> - リソースを共有すると、そのリソースを作成した AWS アカウント 以外のプリンシパルもそれを使用できるようになります。共有しても、リソースを作成したアカウントのリソースに適用されるアクセス許可は変わりません。
> - AWS WA Tool はリージョンサービスです。共有先のプリンシパルは、リソース共有が作成された AWS リージョン 内のみのアクセスが可能です。
> - 2019 年 3 月 20 日以降に開設されたリージョンでリソースを共有するには、自分と共有済みの AWS アカウント の両方が AWS Management Console でそのリージョンを有効にする必要があります。詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS Organizations 内でリソース共有を有効にする

アカウントが AWS Organizations によって管理されている場合、それを活用すればリソースを共有しやすくなります。組織の有無にかかわらず、ユーザーは個々のアカウントに共有できます。ただし、アカウントが組織内にある場合には、各アカウントを列挙しなくても、個々のアカウント、または組織内または OU 内のすべてのアカウントとの共有が可能です。

組織内でリソースを共有するには、まず AWS WA Tool コンソールまたは AWS Command Line Interface (AWS CLI) を使用して AWS Organizations との共有を有効にする必要があります。組織内でリソースを共有する場合、AWS WA Tool はプリンシパルに招待を送信しません。組織内のプリンシパルは、招待状を交換せずに共有リソースにアクセスできます。

組織内でリソースの共有を有効にする場合、AWS WA Tool は `AWSServiceRoleForWellArchitected` と呼ばれるサービスがリンクされたロールを作成します。このロールは AWS WA Tool サービスのみに適用でき、AWS マネージドポリシー `AWSWellArchitectedOrganizationsServiceRolePolicy` を使用して、そのサービスが所属する組織に関する情報を取得する AWS WA Tool アクセス許可を付与します。

組織全体または OU とリソースを共有する必要がなくなった場合は、リソース共有を無効にできます。

要件

- これらの手順は、組織の管理アカウントのプリンシパルとしてサインインしている場合のみ実行できます。
- その組織で、すべての機能が有効になっている必要があります。詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。

> **Important**
>
> AWS WA Tool コンソールを使用して AWS Organizations との共有を有効にする必要があります。これにより、`AWSServiceRoleForWellArchitected` サービスにリンクされたロールが確実に作成されます。AWS Organizations コンソールまたは enable-aws-service-access AWS CLI コマンドを使用して AWS Organizations への信頼されたアクセスを有効にすると、`AWSServiceRoleForWellArchitected` サービスにリンクされたロールが作成されず、組織内でリソースを共有できなくなります。

組織内でリソース共有を有効にするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。

   組織の管理アカウントのプリンシパルとしてサインインしている必要があります。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [AWS Organizations のサポートを有効化] を選択します。
4. [設定を保存] を選択します。

組織内でリソース共有を無効にするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。

   組織の管理アカウントのプリンシパルとしてサインインしている必要があります。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [AWS Organizations のサポートを有効化] を選択解除します。
4. [設定を保存] を選択します。

AWS WA Tool リソースのタグ付け

AWS WA Tool リソースを管理しやすくするために、タグ形式で各リソースに独自のメタデータを割り当てることができます。このトピックでは、タグとその作成方法について説明します。

目次

タグの基本

タグとは、AWS リソースに割り当てるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもお客様側が定義します。

タグを使用すると、AWS リソースを目的、所有者、環境などで分類できます。同じ型のリソースが多い場合に、割り当てたタグに基づいて特定のリソースをすばやく識別できます。たとえば、AWS WA Tool サービスに一連のタグを定義して、各サービスの所有者とスタックレベルを追跡できます。リソースタイプごとに一貫した一連のタグキーを考案することをお勧めします。

タグは自動的にはリソースに割り当てられません。タグを追加したら、いつでもタグキーと値は編集でき、タグはリソースからいつでも削除できます。リソースを削除すると、リソースのタグも削除されます。

タグには、AWS WA Tool に関連する意味はなく、完全に文字列として解釈されます。タグの値を空の文字列に設定することはできますが、タグの値を null に設定することはできません。特定のリソースについて既存のタグと同じキーを持つタグを追加した場合、以前の値は新しい値によって上書きされます。

AWS Management Console、AWS CLI、および AWS WA Tool API を使用してタグを操作できます。

AWS Identity and Access Management (IAM) を使用している場合は、タグを作成、編集、削除するためのアクセス許可を持つ AWS アカウントのユーザーを制御できます。

リソースのタグ付け

新しいまたは既存の AWS WA Tool リソースにタグを付けることができます。

AWS WA Tool コンソールを使用している場合、新しいリソースには作成時にタグを適用でき、既存のリソースにはいつでもタグを適用できます。既存のワークロードには、[プロパティ] タブからタグを適用できます。既存のカスタムレンズ、プロファイル、レビューテンプレートには、[概要] タブからタグを適用できます。

AWS WA Tool API、AWS CLI、または AWS SDK を使用している場合、新しいリソースには、関連する API アクションの `tags` パラメータを使用してタグを適用でき、既存のリソースには、`TagResource` API アクションを使用してタグを適用できます。詳細については、「TagResource」を参照してください。

リソース作成アクションによっては、リソースの作成時にリソースのタグを指定できます。リソースの作成時にタグを適用できない場合、リソースの作成プロセスは失敗します。これにより、作成時にタグ付けするリソースが、指定したタグで作成されるか、まったく作成されないことが確認されます。作成時にリソースにタグを付ける場合、リソースの作成後にカスタムのタグ付けスクリプトを実行する必要はありません。

次の表では、タグ付け可能な AWS WA Tool リソースと、作成時にタグ付け可能なリソースについて説明します。

AWS WA Tool リソースのタグ付けのサポート

リソース	タグをサポート	タグの伝播をサポート	作成時のタグ付けをサポート (AWS WA Tool API、AWS CLI、AWS SDK)
AWS WA Tool ワークロード	はい	いいえ	はい
AWS WA Tool カスタムレンズ	はい	いいえ	はい
AWS WA Tool プロファイル	はい	いいえ	はい

リソース	タグをサポート	タグの伝播をサポート	作成時のタグ付けをサポート (AWS WA Tool API、AWS CLI、AWS SDK)
AWS WA Tool レビューテンプレート	はい	いいえ	はい

タグの制限

タグには以下のような基本制限があります。

- リソースあたりのタグの最大数 - 50 件
- タグキーは、リソースごとにそれぞれ一意である必要があります。また、各タグキーに設定できる値は 1 つのみです。
- キーの最大長 - UTF-8 の 128 Unicode 文字
- 値の最大長 - UTF-8 の 256 Unicode 文字
- 複数の AWS サービス間およびリソース間でタグ付けスキーマを使用する場合、他のサービスでも許可される文字に制限が適用されることがあるのでご注意ください。一般的に使用が許可される文字は、UTF-8 で表現できる文字、数字、スペース、および +、-、=、.、_、:、/、@。
- タグのキーと値は大文字と小文字が区別されます。
- `aws:`、`AWS:`、またはその大文字または小文字の組み合わせを、キーまたは値のプレフィックスとして使用しないでください。これらの文字列は AWS による使用のために予約されています。このプレフィックスが含まれるタグのキーや値を編集したり削除することはできません。このプレフィックスを持つタグは、リソースあたりのタグ数の制限時には計算されません。

コンソールでのタグの処理

AWS WA Tool コンソールを使用すると、新しいリソースまたは既存のリソースに関連付けられたタグを管理できます。

作成時に個々のリソースにタグを追加する

リソースを作成時に AWS WA Tool リソースにタグを追加できます。

個々のリソースでタグを追加および削除する

AWS WA Tool を使用すると、ワークロードの [プロパティ] タブおよびカスタムレンズ、プロファイル、レビューテンプレートの [概要] タブから直接リソースに関連付けられているタグを追加または削除できます。

ワークロードのタグを追加または削除するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Workloads] (ワークロード) を選択します。
4. 修正するワークロードを選択し、[Properties] (プロパティ) を選択します。
5. [タグ] セクションで、[タグを管理] を選択します。
6. 必要に応じてタグを追加または削除します。
   - タグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) のフィールドに入力します。
   - タグを削除するには、[削除] を選択します。
7. 追加、変更、削除を行うタグごとにこのプロセスを繰り返します。[保存] を選択して変更を保存します。

カスタムレンズのタグを追加または削除するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [カスタムレンズ] を選択します。
4. 変更するカスタムレンズの名前を選択します。
5. [概要] タブの [タグ] セクションで、[タグを管理] を選択します。
6. 必要に応じてタグを追加または削除します。
   - タグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) のフィールドに入力します。
   - タグを削除するには、[削除] を選択します。

7. 追加、変更、削除を行うタグごとにこのプロセスを繰り返します。[保存] を選択して変更を保存します。

プロファイルでタグを追加または削除するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [プロファイル] を選択します。
4. 修正するプロファイルの名前を選択します。
5. [概要] タブの [タグ] セクションで、[タグを管理] を選択します。
6. 必要に応じてタグを追加または削除します。
   - タグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) のフィールドに入力します。
   - タグを削除するには、[削除] を選択します。
7. 追加、変更、削除を行うタグごとにこのプロセスを繰り返します。[保存] を選択して変更を保存します。

レビューテンプレートでタグを追加または削除するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [レビューテンプレート] を選択します。
4. 変更するレビューテンプレートの名前を選択します。
5. [概要] タブの [タグ] セクションで、[タグを管理] を選択します。
6. 必要に応じてタグを追加または削除します。
   - タグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) のフィールドに入力します。
   - タグを削除するには、[削除] を選択します。
7. 追加、変更、削除を行うタグごとにこのプロセスを繰り返します。[保存] を選択して変更を保存します。

API を使用したタグの操作

リソースのタグの追加、更新、リスト表示、および削除には、次の AWS WA Tool API オペレーションを使用します。

AWS WA Tool リソースのタグ付けのサポート

タスク	API アクション
1 つ以上のタグを追加、または上書きします。	TagResource
1 つ以上のタグを削除します。	UntagResource
リソースのタグを一覧表示します。	ListTagsForResource

一部のリソース作成アクションでは、リソースの作成時にタグを指定できます。以下のアクションでは、作成時のタグ付けがサポートされます。

タスク	API アクション
ワークロードの作成	CreateWorkload
新しいレンズをインポートする	ImportLens
プロファイルを作成する	CreateProfile
レビューテンプレートを作成する	CreateReviewTemplate

AWS WA Tool による AWS CloudTrail API コールのログ記録

AWS Well-Architected Tool は AWS CloudTrail という、AWS WA Tool の ユーザー、ロール、または AWS のサービスが実行したアクションを記録するサービスと統合しています。CloudTrail は、AWS WA Tool のすべての API コールをイベントとしてキャプチャします。キャプチャされたコールには、AWS WA Tool コンソールのコールと、AWS WA Tool API オペレーションへのコードのコールが含まれます。証跡を作成する場合は、AWS WA Tool のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます 証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail が収集した情報を使用して、AWS WA Tool に対して行われた要求、要求が行われた IP アドレス、要求を行った人、要求が行われた日時、および追加の詳細を判別できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail での AWS WA Tool 情報

CloudTrail は、アカウント作成時に AWS アカウント で有効になります。AWS WA Tool でアクティビティが発生すると、そのアクティビティは [Event history] (イベント履歴) の他の AWS のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウント で表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

AWS WA Tool のイベントなど、AWS アカウント のイベントの継続的な記録に対して、追跡を作成します。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョン に適用されます 証跡は、AWS パーティションのすべてのリージョンからのイベントを口グに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail 口グで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS のサービスを設定できます。詳細については、次を参照してください。

- 追跡を作成するための概要
- CloudTrail のサポート対象サービスと統合
- Amazon SNS の CloudTrail の通知の設定
- [複数のリージョンから CloudTrail ログファイルを受け取る] および [複数のアカウントから CloudTrail ログファイルを受け取る]

すべての AWS WA Tool アクションは CloudTrail によってログに記録され、AWS Well-Architected Toolで定義されたアクションに記録されます。例えば、CreateWorkload、DeleteWorkload、CreateWorkloadShare の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- ユーザーまたはルートユーザーの認証情報のどちらを使用してリクエストが送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

AWS WA Tool ログファイルエントリの理解

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、CreateWorkloadアクションを示す CloudTrail ログエントリです。

```
   {
    "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

Well-Architected リソースに対してアクションが実行されると、AWS Well-Architected Tool は、Amazon EventBridge にイベントを送信します。EventBridge およびこれらのイベントを使用すると、リソースが変更されたときに通知を送信するなどのアクションを実行するルールを記述できます。詳細については、「Amazon EventBridge とは」を参照してください。

> **Note**
>
> イベントは、ベストエフォートベースで送信されます。

次のアクションにより、EventBridge イベントが発生します。

- ワークロード関連
  - ワークロードの作成または削除
  - マイルストーンの作成
  - ワークロードのプロパティの更新
  - ワークロードの共有または共有解除
  - 共有の招待ステータスの更新
  - タグの追加と削除
  - 回答の更新
  - レビューノートの更新
  - ワークロードからのレンズの追加または削除
- レンズ関連
  - カスタムレンズのインポートまたはエクスポート
  - カスタムレンズの公開
  - カスタムレンズの削除
  - カスタムレンズの共有または共有解除
  - 共有の招待ステータスの更新
  - ワークロードからのレンズの追加または削除

AWS WA Tool からのイベント例

このセクションでは、AWS Well-Architected Tool からのイベント例を示します。

ワークロード内の回答の更新


```
{
  "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"
   }
}
```

カスタムレンズの公開

```
{
   "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"
   }
}
```

ドキュメント履歴

次の表は、 AWS Well-Architected Toolの今回のリリースのドキュメントをまとめたものです。

- API バージョン: 最新
- ドキュメントの最新更新日:2024 年 4 月 16 日

変更	説明	日付
Jira	このリリースでは Jira AWS Well-Architected Tool 用コネクタが追加されました。	2024 年 4 月 16 日
新しいレンズ	このリリースでは、レンズカタログに新しいレンズが追加されました。	2024 年 3 月 26 日
更新された機能	このリリースでは、 AWS WA Toolにレンズカタログ機能が追加されました。	2023 年 11 月 26 日
更新された機能	このリリースでは、 AWS WA Toolレビューテンプレート機能がに追加されました。	2023 年 10 月 3 日
WellArchitectedConsoleReadOnlyAccess 管理ポリシーが更新されました。	`"wellarchitected:ExportLens"` が `WellArchitectedConsoleReadOnlyAccess` に追加されました。	2023 年 6 月 22 日
更新された機能	このリリースでは、 AWS WA Toolにプロファイル機能が追加されました。	2023 年 6 月 13 日
更新された機能	このリリースでは、 AWS Trusted Advisor AWS Service	2023 年 5 月 3 日

	Catalog AppRegistry との統合が強化され、`AWSWellArchitectedDiscoveryServiceRolePolicy` AWS が管理ポリシーに追加されました。	
コンテンツの更新	[ダッシュボード] ページが更新され、リスクと改善計画の詳細情報が含まれるようになりました。統合ワークロードレポートを作成する機能も追加されました。	2023 年 3 月 30 日
コンテンツの更新	WellArchitectedConsoleReadOnlyAccess ポリシーの名前が修正されました。	2023 年 1 月 19 日
の IAM ガイダンスを更新しました。 AWS WA Tool	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。	2023 年 1 月 4 日
更新された機能	このリリースでは、FTR レンズがツールから削除されました。	2022 年 12 月 14 日
更新された機能	このリリースでは、 AWS Trusted Advisor AWS Service Catalog AppRegistry と統合が追加されています。	2022 年 11 月 7 日
コンテンツの更新	`choices` のカスタムレンズ JSON の例の問題を修正しました。	2022 年 9 月 29 日

コンテンツの更新	カスタムレンズ JSON 仕様の choices セクションが更新されました。	2022 年 8 月 2 日
更新された機能	このリリースでは、 AWS 管理ポリシーの変更を追跡できるほか、ListAWSServiceAccessForOrganization にアクセス許可を付与する新しいアクションが追加されましたAWSWellArchitectedOrganizationsServiceRolePolicy 。	2022 年 7 月 22 日
組織共有が追加されました	このリリースでは、ワークロードやカスタムレンズを組織や組織部門 (OU) と共有する機能が追加されました。	2022 年 6 月 30 日
更新された機能	このリリースでは、カスタムレンズの選択肢に追加リソースを指定する機能、公開前にカスタムレンズをプレビューする機能、カスタムレンズにタグを追加する機能が追加されました。	2022 年 6 月 21 日
更新された機能	このリリースでは、re: POST の AWS Well-Architected コミュニティにアクセスする機能が追加されました。 AWS	2022 年 5 月 31 日
更新された機能	このリリースでは、チュートリアルにサステナビリティの柱とマイナーアップデートが追加されました。	2022 年 3 月 31 日

EventBridge サポートが追加されました	AWS WA Tool Well-Architected EventBridge リソースに変更が加えられると、Amazon にイベントを送信するようになりました。	2022 年 3 月 3 日
カスタムレンズの追加	カスタムレンズを追加する機能が追加されました。	2021 年 11 月 29 日
更新された機能	個々のベストプラクティスを適用しないものとしてマークできるようになりました。	2021 年 7 月 14 日
リソースへのタグ付けが可能に	このリリースでは、ワークロードにタグを追加する機能が追加されました。	2021 年 3 月 3 日
API の提供を開始	このリリースでは API が追加されました。 AWS WA Tool AWS CloudTrail ロギング情報が追加されました。	2020 年 12 月 16 日
更新された機能	このリリースでは、FTR レンズと SaaS レンズがツールに追加されました。	2020年12月3日
データ保護の更新	データ保護情報が更新されました。	2020 年 11 月 5 日
コンテンツの更新	新しいレンズを使用するようにワークロードをアップグレードした後、以前のバージョンに戻すことはできないことを明確化しました。	2020年7月8日
コンテンツの更新	2019 年 3 月 20 AWS リージョン 日以降に導入された共有を明確化しました。	2020 年 6 月 24 日

更新された機能	ワークロード共有への招待が拒否されると、ワークロード共有へのアクセスはすぐに削除されます。共有が承諾されると、共有アクセスが許可されます。	2020 年 6 月 17 日
コンテンツの更新	高リスクの問題 (HRI) と中リスクの問題 (MRI) の定義を追加しました。	2020 年 6 月 12 日
コンテンツの更新	AWS データの使用方法に関するセクションが追加されました。	2020 年 5 月 21 日
更新された機能	このリリースでは、レビュー所有者がワークロードに追加されます。	2020 年 4 月 1 日
更新された機能	このリリースでは、ワークロードにアーキテクチャ図のリンクが追加されます。	2020 年 3 月 10 日
コンテンツの更新	AWS リージョンワークロードシェアは特定のものであることが明記されました。	2020 年 1 月 10 日
更新された機能	このリリースでは、ワークロードの共有を追加しました。	2020年1月9日
コンテンツの更新	セキュリティセクションが最新のガイダンスで更新されました。	2019 年 12 月 6 日

更新された機能	このリリースでは、ワークロードを定義するときに [業界] フィールドがオプションになります。	2019 年 8 月 19 日
更新された機能	このリリースでは、ワークロードレポートに改善計画項目が追加されました。	2019 年 7 月 29 日
更新された機能	このリリースでは、DeleteWorkload ポリシーにアクションが追加されました。	2019 年 7 月 18 日
コンテンツの更新	このガイドの内容は、わずかな修正を加えて更新されました。	2019 年 6 月 19 日
コンテンツの更新	このガイドの内容は、わずかな修正を加えて更新されました。	2019 年 5 月 30 日
更新された機能	このリリースでは、ワークロードレビューに使用されるフレームワークのバージョンのアップグレードがサポートされました。	2019 年 5 月 1 日
更新された機能	このリリースでは、AWS リージョン ワークロードを定義する際にnon--を指定する機能が追加されました。	2019 年 2 月 14 日
AWS Well-Architected Tool 一般提供開始	このリリースでは、 AWS Well-Architected Toolが導入されました。	2018 年 11 月 29 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。